

HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide

for HP Integrated Lights-Out versions 1.82 and 1.91 and HP Integrated Lights-Out 2 versions 1.1x, 1.2x, 1.3x, 1.70, 1.75, and 1.77



© Copyright 2005, 2009 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Microsoft, Windows, Windows Server, Windows Vista, Windows NT, and Windows XP are U.S. registered trademarks of Microsoft Corporation. AMD is a trademark of Advanced Micro Devices, Inc. Intel is a trademark of Intel Corporation in the U.S. and other countries. Java is a U.S. trademark of Sun Microsystems, Inc.

Intended audience

This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Contents

Introduction	7
Guide overview	7
New in this version	7
HP ProLiant Essentials Rapid Deployment Pack Integration	8
Server management through IPMI version 2.0 compliant applications	8
WS-Management compatibility overview	9
Command line	10
Command line interface overview	10
Command line access	10
Using the command line	10
Escape commands	12
Base commands	12
Specific commands	13
User commands	14
HP SIM SSO settings	15
Network commands	16
iLO 2 settings	19
iLO 2 embedded health settings	20
SNMP settings	22
License commands	23
Directory commands	23
Virtual media commands	25
Start and reset commands	27
Firmware update	29
Eventlog commands	29
Blade commands	30
Boot commands	31
LED commands	32
System properties and targets	32
Other commands	35
Telnet	36
Telnet support	36
Using Telnet	36
Telnet simple command set	36
Telnet security	37
Supported key sequences	37
iLO 2 VT100+ key map	37
VT100+ codes for the F-keys	40
Linux codes for the F-keys	40
Secure Shell	41
SSH overview	41
SSH features supported by iLO 2	41
Using Secure Shell	42
SSH key authorization	42

Tool definition files.....	43
Mxagentconfig.....	43
Importing SSH keys from PuTTY.....	43
Importing SSH keys generated using ssh-keygen.....	45
Group administration and iLO 2 scripting.....	46
Lights-Out Configuration Utility.....	46
Unauthenticated XML query.....	46
Query definition in HP SIM.....	47
Application Launch using HP SIM.....	47
Batch processing using the Lights-Out Configuration Utility.....	48
Lights-Out Configuration Utility parameters.....	49
Perl scripting.....	51
Using Perl with the XML scripting interface.....	51
XML enhancements.....	51
Opening an SSL connection.....	52
Sending the XML header and script body.....	53
Virtual Media scripting.....	55
Scripting Web server requirements.....	55
Using virtual media scripting.....	55
Using Virtual Media on Linux servers through an SSH connection.....	56
Virtual media image files.....	57
CGI helper application.....	57
Setting up IIS for scripted virtual media.....	58
HPONCFG online configuration utility.....	61
HPONCFG.....	61
HPONCFG supported operating systems.....	61
HPONCFG requirements.....	61
Installing HPONCFG.....	62
Windows server installation.....	62
Linux server installation.....	62
HPONCFG utility.....	62
HPONCFG command line parameters.....	63
Obtaining the basic configuration.....	64
Obtaining a specific configuration.....	65
Setting a configuration.....	66
Using variable substitution.....	67
Capturing and restoring a configuration.....	67
Using RIBCL.....	70
Overview of the RIBCL.....	70
XML header.....	70
Data types.....	70
Response definitions.....	71
RIBCL.....	71
RIBCL parameters.....	71
RIBCL runtime errors.....	71
LOGIN.....	72
LOGIN parameters.....	72
LOGIN runtime errors.....	72
USER_INFO.....	72
ADD_USER.....	73

DELETE_USER.....	75
DELETE_CURRENT_USER.....	75
GET_USER.....	76
MOD_USER.....	77
GET_ALL_USERS.....	79
GET_ALL_USER_INFO.....	80
RIB_INFO.....	81
RESET_RIB.....	82
GET_EVENT_LOG.....	82
CLEAR_EVENTLOG.....	84
COMPUTER_LOCK_CONFIG.....	84
GET_NETWORK_SETTINGS.....	86
MOD_NETWORK_SETTINGS.....	87
GET_GLOBAL_SETTINGS.....	91
MOD_GLOBAL_SETTINGS.....	93
GET_SNMP_IM_SETTINGS.....	98
MOD_SNMP_IM_SETTINGS.....	99
UPDATE_RIB_FIRMWARE.....	100
GET_FW_VERSION.....	101
HOTKEY_CONFIG.....	102
LICENSE.....	104
INSERT_VIRTUAL_MEDIA.....	104
EJECT_VIRTUAL_MEDIA.....	106
GET_VM_STATUS.....	106
SET_VM_STATUS.....	107
CERTIFICATE_SIGNING_REQUEST.....	109
IMPORT_CERTIFICATE.....	109
GET_TWOFACOR_SETTINGS.....	110
MOD_TWOFACOR_SETTINGS.....	111
DIR_INFO.....	113
GET_DIR_CONFIG.....	114
IMPORT_SSH_KEY.....	115
MOD_DIR_CONFIG.....	116
RACK_INFO.....	119
GET_RACK_SETTINGS.....	119
GET_DIAGPORT_SETTINGS.....	120
MOD_DIAGPORT_SETTINGS.....	120
GET_ENCLOSURE_IP_SETTINGS.....	122
MOD_ENCLOSURE_IP_SETTINGS.....	123
GET_TOPOLOGY.....	124
MOD_BLADE_RACK.....	124
SERVER_INFO.....	126
GET_SERVER_NAME.....	127
SERVER_NAME.....	127
GET_EMBEDDED_HEALTH.....	128
GET_POWER_READINGS.....	130
GET_POWER_CAP.....	131
SET_POWER_CAP.....	131
GET_HOST_POWER_SAVER_STATUS.....	132
SET_HOST_POWER_SAVER.....	133
GET_HOST_POWER_REG_INFO.....	134
GET_HOST_POWER_STATUS.....	135
SET_HOST_POWER.....	136

GET_HOST_PWR_MICRO_VER	136
GET_PWREG_CAPABILITIES.....	137
RESET_SERVER.....	139
PRESS_PWR_BTN	140
HOLD_PWR_BTN	140
COLD_BOOT_SERVER	141
WARM_BOOT_SERVER	141
SERVER_AUTO_PWR	142
GET_SERVER_AUTO_PWR.....	143
GET_UID_STATUS	143
UID_CONTROL.....	144
GET_VPB_CABLE_STATUS (RiLOE II only).....	144
SSO_INFO.....	145
GET_SSO_SETTINGS.....	146
MOD_SSO_SETTINGS.....	147
SSO_SERVER.....	149
DELETE_SERVER	150
HPQLOMGC command language	152
Using HPQLOMGC	152
ILO_CONFIG	152
iLO 2 ports.....	154
Enabling the iLO 2 Shared Network Port feature through XML scripting	154
Re-enabling the dedicated NIC management port.....	154
iLO 2 parameters.....	156
Status Summary parameters.....	156
User Administration parameters.....	157
Global Settings parameters.....	158
Network parameters	162
Network DHCP/DNS parameters	163
SNMP/Insight Manager settings parameters	164
Directory settings parameters	165
BL p-Class parameters	166
iLO Advanced Pack License Key.....	168
Technical support.....	169
HP contact information.....	169
Before you contact HP.....	169
Acronyms and abbreviations.....	170
Index.....	176

Introduction

Guide overview

HP iLO 2 provides multiple ways to configure, update, and operate HP ProLiant servers remotely. The *HP Integrated Lights-Out User Guide* and the *HP Integrated Lights-Out 2 User Guide* describe each feature and explain how to use these features with the browser-based interface and RBSU.

The *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* describes the syntax and tools available to use iLO 2 through a command line or scripted interface.

Sample XML scripts downloaded from the HP website contain commands for all iLO, iLO 2, and RILOE II firmware. Unless otherwise specified, examples in this guide are specifically for iLO 2 firmware version 1.10 and later. Before using the XML sample scripts downloaded from the HP website (<http://h18004.www1.hp.com/support/files/lights-out/us/index.html>), read the firmware support information in each sample script to tailor the script for the intended firmware and version.

New in this version

This guide reflects changes in the iLO 2 firmware. This guide covers iLO versions 1.82, 1.91, and iLO 2 versions 1.1x, 1.2x, 1.30, 1.70, 1.75, and 1.77. This version of the guide includes updates for the following:

- Sections:
 - "HPONCFG online configuration utility (on page 61)"
 - "Directory commands (on page 23)"
 - "Blade commands (on page 30)"
 - "Boot commands (on page 31)"
 - "System properties and targets (on page 32)"
 - "Group administration and iLO 2 scripting (on page 46)"
- Updated the following RIBCL commands:
 - UPDATE_RIB_FIRMWARE
 - GET_HOST_PWR_MICRO_VER
 - GET_PWREG_CAPABILITIES

For information about these updates, see "Using RIBCL (on page 70)."

HP ProLiant Essentials Rapid Deployment Pack Integration

HP ProLiant Essentials Rapid Deployment Pack integrates with iLO 2 to allow the management of remote servers and the performance of remote console operations regardless of the state of the operating system or hardware.

The Deployment Server provides the ability to use the power management features of iLO 2 to power on, power off, or cycle power on the target server. Each time a server connects to the Deployment Server, the Deployment Server polls the target server to see if a LOM management device is installed. If installed, the server gathers information including the DNS name, IP address, and first user name. Security is maintained by requiring the user to enter the correct password for that user name.

For more information about the ProLiant Essentials Rapid Deployment Pack, refer to the documentation that ships on the ProLiant Essentials Rapid Deployment Pack CD or the HP website (<http://www.hp.com/servers/rdp>).

Server management through IPMI version 2.0 compliant applications

Server management through the IPMI is a standardized method for controlling and monitoring the server. iLO 2 provides server management based on the IPMI version 2.0 specification.

The IPMI specification defines a standardized interface for platform management. The IPMI specification defines the following types of platform management:

- Monitoring of system information, such as fans, temperatures, and power supplies
- Recovery capabilities, such as system resets and power on/off operations
- Logging capabilities, for abnormal events such as over temperature readings or fan failures
- Inventory capabilities, such as identifying failed hardware components

IPMI communications are dependent on the BMC and the SMS. The BMC manages the interface between the SMS and the platform management hardware. iLO 2 emulates the BMC functionality and the SMS functionality can be provided by various industry-standard tools. For additional information, see the IPMI specification on the Intel® website (<http://www.intel.com/design/servers/ipmi/tools.htm>).

iLO 2 provides the KCS interface, or open interface, for SMS communications. The KCS interface provides a set of I/O mapped communications registers. The default system base address for the I/O mapped SMS Interface is 0xCA2 and is byte aligned at this system address.

The KCS interface is accessible to SMS software that is running on the local system. Examples of compatible SMS software applications are as follows:

- IPMI version 2.0 Command Test Tool is a low-level MS-DOS command line tool that enables hex-formatted IPMI commands to be sent to an IPMI BMC that implements the KCS interface. You can locate this tool on the Intel® website (<http://www.intel.com/design/servers/ipmi/tools.htm>).
- IPMITool is a utility for managing and configuring devices that support the IPMI version 1.5 and version 2.0 specifications and can be used in a Linux environment. You can locate this tool on the IPMITool website (<http://ipmitool.sourceforge.net/index.html>).

IPMI functionality provided by iLO 2

When emulating a BMC for the IPMI interface, iLO 2 supports all mandatory commands listed in the IPMI version 2.0 specification. See the IPMI version 2.0 specification for a listing of these commands. Also, the SMS should use the methods described in the specification for determining which IPMI features are enabled or disabled in the BMC (for example, using the Get Device ID command).

If the server operating system is running and the health driver is enabled, any IPMI traffic through the KCS interface can affect the performance of the health driver and overall health performance of the system. Do not issue any IPMI commands through the KCS interface that could have a detrimental affect on the monitoring performed by the health driver. These commands include any commands that sets or changes IPMI parameters, such as `Set Watchdog Timer` and `Set BMC Global Enabled`. Any IPMI command that simply returns data is safe to use, such as `Get Device ID` and `Get Sensor Reading`.

WS-Management compatibility overview

The iLO 2 firmware implementation of WS-Management is in accordance with the specification, DTMF *Web Services for Management 1.0.0a*.

Authentication

- iLO 2 uses basic authentication over SSL, compliant with profile:
`wsman:secprofile/https/basic`
- Authenticated users are authorized to execute WS-Management commands in accordance with designated privileges in their local or directory accounts.
- To enable basic authentication on Microsoft® Windows Vista™, at the command prompt, enter `gpedit.msc` to launch the Group Policy Object Editor. Select **Computer Configuration> Administrative Templates> Windows Components> Windows Remote Management (WinRM)> WinRM Client**. Set Allow Basic authentication to **Enabled**.

Compatibility

- WS-Management in iLO 2 are compatible with the Windows Vista™ WinRM utility, Microsoft® Operations Manager 3, and the Management Pack provided by HP.
- The full set of WS-Management commands is available on iLO 2 servers that support embedded system health. A greatly reduced subset of these commands is available on servers without embedded systems health support.

Commands are available for remote invocation of the following devices:

- Server power
- UID

Status

The WS-Management in iLO 2 returns status information for fans, temperatures, power supplies, and VRMs.

Command line

Command line interface overview

HP has worked with key industry partners within Distributed Management Task Force, Inc. to define an industry-standard set of commands. DMTF is working on a suite of specifications, Systems Management Architecture for Server, to standardize manageability interfaces for servers. The iLO 2 uses the command set defined in the *Server Management Command Line Protocol Specification, 1.00 Draft*. The CLP is intended to replace the simple CLI.

Command line access

The iLO 2 features enable you to execute the supported commands from a command line. There are two interfaces through which the command line option can be accessed:

- Serial port using one connection
- Network using:
 - SSH enabling three simultaneous connections. IP address or DNS name, login name, and password are required to start a session using SSH.
 - Telnet protocol using three simultaneous connections.

Any four network connections can be active simultaneously. After serial CLI is enabled on the Global Settings screen, the iLO 2 CLI is invoked by entering `ESC` (. The SSH and Telnet sessions start the after authentication.

Using the command line

After initiating a command line session, the iLO 2 CLI prompt appears. Each time a command is executed (or you exit the Remote Console or VSP) you will be returned to the CLI prompt as shown in the following example.

```
hpiLO->
```

Each time a CLI command is executed, the returned output follows this general format:

```
hpiLO-> {CLI command}
status=0
status_tag=COMMAND COMPLETED
... output returned...
```

```
hpiLO->
```

If an invalid command is entered, then the status and status_tag values reflects the error as shown:

```
hpiLO-> boguscommand
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND NOT RECOGNIZED
```

If an invalid parameter is given to a valid command, the response is slightly different:

```
hpiLO-> show /bad
status=2
status_tag=COMMAND PROCESSING FAILED
error_tag=COMMAND ERROR-UNSPECIFIED
Invalid property.
```

```
hpiLO->
```

The following commands are supported in this release of CLP. The same command set is supported through the serial port, SSH, and telnet connections.

The privilege level of the logged in user is checked against the privilege required for the command. The command is only executed if the privilege levels match. If the serial command line session status is set to Enabled-No Authentication, then all the commands are executed without checking the privilege level.

The general syntax of CLP command is:

```
<verb> <target> <option> <property>
```

- **Verbs**—The supported verbs are:
 - cd
 - create
 - delete
 - help
 - load
 - reset
 - set
 - show
 - start
 - stop
 - exit
 - version
- **Target**—The default target is the /. The target can be changed by the cd command or by specifying a target on the command line.
- **Options**—The valid options are:
 - -help/-h
 - -all/-a
- **Properties** are the attributes of the target that can be modified.
- **Output**—The output syntax is:
 - status
 - status_tag
 - status_msg

The valid Boolean values for any command are yes, no, true, false, y, n, t, and f.

General notes

If the commands on the CLP command span more than one line, you cannot navigate between different lines.

Operating system-specific notes:

- Windows® 2000 telnet client does not support the Functions keys F1,..., F12, Insert, Home, and End keys. These keys do not work in an iLO 2 command line session.
- The Backspace key in iLO 2 CLP implementation is mapped to the value 0x8. Some client operating systems such as, Novell Linux Desktop and Red Hat Enterprise Linux 4 Desktop map the Backspace key to the value 0x7f, which is used for the Delete key in Windows® telnet client. The Backspace key does not work from a client where it has value of 0x7f. For the Linux clients, using the Home or the End key enables the iLO 2 CLP service to remap the Backspace key to use the value 0x7f, making the key functional.

In the Windows® PuTTY client, the Backspace key can be mapped to a value of 0x8 by changing the setting for Terminal Keyboard to Control-H.

Escape commands

The escape key commands are short-cuts to popular tasks.

- `ESC (` invokes the serial CLI connection. This is not necessary for SSH or telnet sessions because they automatically start a CLI session after a successful login.
- `ESC Q` stops the CLI session and terminates the SSH and telnet connection.
- `ESC R ESC r ESC R` resets the system.
- `ESC ^` powers on the system.
- `ESC ESC` erases the current line.

There is a one second timeout for entering any of the escape sequence characters.

Base commands

- The `help` command displays context-sensitive help.
Entering `help` displays all supported commands. Entering `<command help/?>` displays the help message specific to that command.
- The `exit` command terminates the CLP session.
- The `cd` command sets the current default target. The context works like a directory path. The root context for the server is "/" and this is the starting point for a CLP system. By changing the context, you can shorten commands.
For example, to find the current iLO 2 firmware version, you could enter the command `show /map1/firmware version`. However, if you enter the `cd /map1/firmware` command, then a simple `show version` command displays the information.
- The `show` command displays values of a property or contents of a collection target. For example:

```
hpiLO-> show
status=0
status_tag=COMMAND COMPLETED

/
Targets
  system1
```

```

    map1
    Properties
    Verbs

    cd version exit show

```

The first line of information returned by the `show` command is the current context. In the example, `/` is the current context. Following the context is a list of subtargets (Targets) and properties (Properties) applicable to the current context. The verbs (Verbs) section shows which commands are applicable to this context.

You can also specify the `show` command with an explicit or implicit context as well as a specific property. For example, an explicit context is `/map1/firmware` and is not dependant on the current context, while an implicit context assumes that the context specified is a child of the current context. If the current context is `/map1` then a `show firmware` command displays the `/map1/firmware` data.

If you do not specify a property, then all properties are shown. In the case of the `/map1/firmware` context, there are two properties available: `version` and `date`. If you execute `show /map1/firmware date`, only the `date` is shown.

- The `create` command creates a new instance of the MAP in the name space.
- The `delete` command removes instances of the MAP in the name space.
- The `load` command moves a binary image from a URL to the MAP.
- The `reset` command causes a target to cycle from enabled to disabled, and back to enabled.
- The `set` command sets a property or set of properties to a specific value, and resets iLO 2 to implement the changes.
- The `start` command causes a target to change its state to a higher run level.
- The `stop` command causes a target to change its state to a lower run level.
- The `version` command queries the version of the CLP implementation or other CLP elements. For example:

```

hpiLO-> version
status=0
status_tag=COMMAND COMPLETED
SM-CLP Version 1.0

```
- The `oemhp_ping` command determines if an IP address is reachable from the current iLO 2. For example :

```

oemhp_ping 192.168.1.1

```

where `192.168.1.1` is the IP address you are testing.

Specific commands

The following sections cover iLO 2 specific commands available when using the command line, including:

- User commands (on page [14](#))
- HP SIM SSO settings (on page [15](#))
- Network commands (on page [16](#))
- iLO 2 settings (on page [19](#))
- iLO 2 embedded health settings (on page [20](#))

- SNMP settings (on page [22](#))
- License commands (on page [23](#))
- Directory commands (on page [23](#))
- Virtual media commands (on page [25](#))
- Start and reset commands (on page [27](#))
- Firmware update (on page [29](#))
- Eventlog commands (on page [29](#))
- Blade commands (on page [30](#))
- Boot commands (on page [31](#))
- LED commands (on page [32](#))
- System targets and properties ("[System properties and targets](#)" on page [32](#))
- Other commands (on page [35](#))

User commands

User commands enable you to view and modify user settings. User settings are located at `/map1/accounts1`.

Targets

All local users are valid targets. For example, if there are three local users with the login names Administrator, admin, and test, then valid targets would be:

- Administrator
- admin
- test

Properties

Property	Access	Description
username	read/write	Corresponds to the iLO 2 login name.
password	read/write	Corresponds to the password for the current user.
name	read/write	Displays the name of the user. If a name is not specified, the parameter uses the same value as the login name (username). This value corresponds to the iLO 2 user name property.

Property	Access	Description
group	read/write	<p>Specifies the privilege level. The valid values are as follows:</p> <ul style="list-style-type: none"> • admin • config • oemhp_power • oemhp_rc • oemhp_vm <p>If a group is not specified, no privileges are assigned to the user.</p>

Examples

The current path is `/map1/accounts1`.

- `create username=lname1 password=password`
In the example, *username* corresponds to the login name.
- `set lname1 username=lname2 password=password1 name=name2 group=admin,configure,oemhp_power,oemhp_vm,oemhp_rc`
In the example, *lname1* is the login name of the user.

HP SIM SSO settings

HP SIM SSO settings commands are accessed using `/map1/oemhp_ssocfg1`. You must have the Configure iLO 2 Settings privilege to change these properties. SSO is only supported for browser access from trusted HP SIM servers. SSO is a licensed feature. See the *HP Integrated Lights-Out User Guide*, for more information.

Targets

None

Properties

Property	Access	Description
oemhp_ssotrust	Read/write	The Single Sign-On required trust level. Valid values are disabled, all, name, and certificate.
oemhp_ssouser	Read/write	The privileges associated with the user role. Valid values are login, oemhp_rc, oemhp_power, oemhp_vm, config, admin

Property	Access	Description
oemhp_ssooperator	Read/write	The privileges associated with the operator role. Valid values are login, oemhp_rc, oemhp_power, oemhp_vm, config, admin.
oemhp_ssadministrator	Read/write	The privileges associated with the administrator role. Valid values are login, oemhp_rc, oemhp_power, oemhp_vm, config, admin.
oemhp_ssoserver	Read	Contains 0 or more HP SIM Trusted Server records. Each record can contain a server name or a server certificate.

Examples

- To set the SSO trust level to trust by certificate:
set oemhp_ssocfg/ oemhp_ssotrust = certificate
- To assign user roles the login privilege:
set oemhp_ssocfg/ oemhp_ssouser = login
- To assign the operator role login, remote console, virtual power control, and virtual media privileges:
set oemhp_ssocfg/ oemhp_ssooperator = login,oemhp_rc,oemhp_power,oemhp_vm
- To Add an HP SIM Trusted Server name record:
cd map1/oemhp_ssocfg
</map1/oemhp_ssocfg>hpiLO-> create = hpsim1.corp.net
- To dynamically import a certificate from the specified server (hpsim2.corp.net):
</map1/oemhp_ssocfg>hpiLO-> load = hpsim2.corp.net
- To delete oemhp_ssoserver with index 5.
</map1/oemhp_ssocfg>hpiLO-> delete = 5
- To display the complete iLO 2 SSO configuration:
cd map1/oemhp_ssocfg
</map1/oemhp_ssocfg>hpiLO->show

Network commands

The network subsystems are located at:

- /map1/enetport1
- /map1/dhccpendpt1

- /map1/dnsendpt1
- /map1/gateway1
- /map1/dnsserver1
- /map1/dnsserver2
- /map1/dnsserver3
- /map1/dhcpserver1
- /map1/settings1
- /map1/vlan1

Properties, Targets, and Verbs:

- dhcpendpt1
 - Properties
 - EnabledState
 - OtherTypeDescription
- dnsendpt1
 - Properties
 - EnabledState
 - HostName
 - DomainName
 - OtherTypeDescription
- gateway1
 - Properties
 - AccessInfo
 - AccessContext
- dnsserver1
 - Properties
 - AccessInfo
 - AccessContext
 - Verbs
 - cd
 - version
 - exit
 - show
 - set
- dnsserver2
 - Properties
 - AccessInfo
 - AccessContext

- dnsserver3
 - Properties
 - AccessInfo
 - AccessContext
- dhcpserver1
 - Properties
 - AccessInfo
 - AccessContext
- settings1
 - Targets
 - DNSSettings1
 - Properties
 - DNSServerAddress
 - RegisterThisConnection
 - DomainName
 - DHCPOptionToUse
 - WINSSettingData1
 - Properties
 - WINSServerAddress
 - RegisterThisConnection
 - DHCPOptionToUse
 - Verbs
 - cd
 - version
 - exit
 - show
 - StaticIPSettings1
 - Properties
 - oemhp_SRoute1Address
 - oemhp_Gateway1Address
 - oemhp_SRoute2Address
 - oemhp_Gateway2Address
 - oemhp_SRoute3Address
 - oemhp_Gateway3Address
 - DHCPOptionToUse

Examples

```
set /map1/enetport1 speed=100
```

```
set /map1/enetport1/lanendpt1 ipv4address=192.168.0.13 subnetmask=255.255.252
```

You can specify one or more properties on the command line. If multiple properties are given on the same command line, they must to be separated by a space.

iLO 2 is reset after network settings have been applied.

iLO 2 settings

The iLO 2 settings commands enable you to view or modify iLO 2 settings. iLO 2 settings are located at /map1/config1.

Targets

No targets

Properties

Property	Access	Description
oemhp_enable	Read/Write	Enables or disables the iLO 2. Boolean values are accepted.
oemhp_timeout	Read/Write	Sets session timeout in minutes. Valid values are 15, 30, 60, and 120.
oemhp_passthrough	Read/Write	Enables or disables Terminal Services Passthrough. Boolean values are accepted.
oemhp_rbsuenable	Read/Write	Enables or disables RBSU prompt during POST. Boolean values are accepted.
oemhp_rbsulogin	Read/Write	Enables or disables login requirement for accessing RBSU. Boolean values are accepted.
oemhp_rbsushowip	Read/Write	Enables or disables iLO 2 IP address display during POST. Boolean values are accepted.
oemhp_rcconfig	Read/Write	Sets the Remote Console configuration. Valid values are enabled, disabled, or automatic.
oemhp_telnetenable	Read/Write	Enables or disables telnet.
oemhp_httpport	Read/Write	Sets the HTTP port value.
oemhp_sslport	Read/Write	Sets the SSL port value.
oemhp_rcport	Read/Write	Sets remote console port value.
oemhp_vmport	Read/Write	Sets virtual media port value.
oemhp_tsport	Read/Write	Sets Terminal Services port value.
oemhp_sshport	Read/Write	Sets the SSH port value.
oemhp_sshstatus	Read/Write	Enables or disables SSH. Boolean values are accepted.
oemhp_serialclstatus	Read/Write	Enables or disables CLP session through serial port. Boolean values are accepted.

Property	Access	Description
oemhp_serialcliath	Read/Write	Enables or disables authorization requirement for CLP session through serial port. Boolean values are accepted.
oemhp_serialclispeed	Read/Write	Sets the serial port speed for the CLP session. The valid values are 9600, 19200, 38400, 57600, and 115200.
oemhp_minpwdlen	Read/Write	Sets the minimum password length requirement.
oemhp_authfailurelogging	Read/Write	Sets the logging criteria for failed authentications.
oemhp_hotkey_t	Read/Write	Sets the value for hotkey Ctrl+T.
oemhp_hotkey_u	Read/Write	Sets the value for hotkey Ctrl+U.
oemhp_hotkey_v	Read/Write	Sets the value for hotkey Ctrl+V.
oemhp_hotkey_w	Read/Write	Sets the value for hotkey Ctrl+W.
oemhp_hotkey_x	Read/Write	Sets the value for hotkey Ctrl+X.
oemhp_hotkey_y	Read/Write	Sets the value for hotkey Ctrl+Y.
oemhp_rc_acquire (not supported in iLO 2 v1.00)	Read/Write	Enables or disables remote console acquire operations.
oemhp_high_perf_mouse	Read/Write	Enables or disables high performance mouse.
oemhp_computer_lock	Read/Write	Enables or disables the Remote Console Computer Lock.
oemhp_enforce_aes	Read/Write	Enable or disable enforcing AES/3DES encryption

Examples

```
set /map1/config1 oemhp_enable=yes oemhp_timeout=30
```

You can specify one or more properties in the command line. If multiple properties are given on the same command line, they must be separated by a space.

`oemhp_computer_lock` command examples:

```
set /map1/config1 oemhp_computer_lock = windows
set /map1/config1 oemhp_computer_lock = custom,l_gui,1
set /map1/config1 oemhp_computer_lock = disabled
```

For a complete list of `oemhp_computer_lock` custom keys, see the *HP Integrated Lights-Out 2 User Guide*. Any keys with a space must have the space replaced with an underscore. For example:

```
set /map1/config1 oemhp_computer_lock = custom,SYS_RQ
set /map1/config1 oemhp_computer_lock = custom,SYS_RQ
```

iLO 2 embedded health settings

iLO 2 embedded health commands enable you to display system embedded health information for fans, temperature sensors, voltage sensors, and the power supply.

iLO 2 embedded health CLP settings are located at `/system1/fan*`, `/system1/sensor*`, and `/system1/powersupply*`.

Targets

- Fan
- Sensor
- Power supply

Properties

Property	Access	Description
DeviceID	Read	Displays fan, sensor, or power supply label number
ElementName	Read	Displays fan, sensor, or power supply location
OperationalStatus	Read	Displays fan, sensor, or power supply operational status
VariableSpeed	Read	Displays if fan is operating at variable speed
Desired Speed	Read	Displays the current fan speed
HealthState	Read	Displays the health status of the fan, sensor, or power supply
RateUnits	Read	Displays the reading units for temperature and voltage sensors
CurrentReading	Read	Displays the current reading of sensor
SensorType	Read	Displays the sensor type
Oemhp_CautionValue	Read	Displays temperature sensor caution value
Oemhp_CriticalValue	Read	Displays temperature sensor critical value

Examples

The command `show system1/fan1` displays the system fan1 properties. For example:

```
/system1/fan1
Targets
Properties
  DeviceID=Fan 1
  ElementName=I/O Board
  OperationalStatus=Ok
  VariableSpeed=Yes
  DesiredSpeed=40
  HealthState=Ok.
```

VRM power supplies are usually mapped to the sensor targets. The command `show system1/sensor1` displays the VRM 1 properties. For example:

```
/system1/sensor1
Targets
Properties
  DeviceID=VRM 1
```

```

ElementName=CPU 1
OperationalStatus=Ok
RateUnits=Volts
CurrentReading=0
SensorType=Voltage
HealthState=Ok
oemhp_CautionValue=0
oemhp_CriticalValue=0

```

Other sensor targets show system temperatures. The command `show system1/sensor3` displays one of the temperature zone properties. For example:

```

/system1/sensor3
Targets
Properties
  DeviceID=Temp 1
  ElementName=I/O Board Zone
  OperationalStatus=Ok
  RateUnits=Celsius
  CurrentReading=32
  SensorType=Temperature
  HealthState=Ok
  oemhp_CautionValue=68
  oemhp_CriticalValue=73

```

SNMP settings

SNMP settings commands enable you to view and modify SNMP settings. SNMP settings are available at `/map1/snmp1`.

Targets

None

Properties

Property	Access	Description
<code>accessinfo1</code>	Read/Write	Sets the first SNMP trap destination address.
<code>accessinfo2</code>	Read/Write	Sets the second SNMP trap destination address.
<code>accessinfo3</code>	Read/Write	Sets the third SNMP trap destination address.
<code>oemhp_iloalert</code>	Read/Write	Enables or disables iLO 2 SNMP alerts. Boolean values accepted.
<code>oemhp_agentalert</code>	Read/Write	Enables or disables host agent SNMP alerts. Boolean values accepted.
<code>oemhp_snmpassthru</code>	Read/Write	Enables or disables iLO 2 SNMP pass-through. Boolean values accepted.
<code>oemhp_imagenturl</code>	Read/Write	Sets the Insight Manager Agent URL.

Property	Access	Description
oemhp_imdatalevel	Read/Write	Determines if the LOM device responds to anonymous XML queries. Valid selections can be enabled and disabled.

Examples

```
set /map1/snmp1 accessinfo1=192.168.0.50 oemhp_imdatalevel=Enabled
```

You can specify one or more properties on the command line. If there are multiple properties on the same command line, they must be separated by a space.

License commands

License commands enable you to display and modify the iLO 2 license. License commands are available at /map1/.

Targets

None

Commands

Command	Description
cd	Changes the current directory
show	Displays license information
set	Changes the current license

Examples

- `set /map1 license=1234500000678910000000001`
- `show /map1 license`

Directory commands

Directory commands enable you to view and modify directory settings. Directory settings are available at: /map1/oemhp_dircfg1

Targets

None

Properties

Property	Access	Description
oemhp_dirauth	Read/Write	Enables or disables directory authentication. Valid settings are as follows: <ul style="list-style-type: none"> extended_schema—Uses HP extended schema default_schema—Uses schema-free directories disabled—Directory-based authentication is disabled
oemhp_localacct	Read/Write	Enables or disables local account authentication. This property can be disabled only if directory authentication is enabled. Boolean values accepted.
oemhp_dirsrvaddr	Read/Write	Sets the directory server IP address or DNS name. The schema-free directory configuration requires a DNS name.
oemhp_ldapport	Read/Write	Sets the directory server port.
oemhp_dirdn	Read/Write	Displays the LOM object distinguished name. This field is ignored when the schema-free directory configuration is used.
oemhp_dirpassword	Read/Write	Sets the LOM object password. This field is ignored when the default schema configuration is used.
oemhp_usercntxt1, 2 ... up to 15	Read/Write	Displays the directory user login search context. This field is not necessary when the schema-free directory configuration is used.
oemhp_group{n}_name where $n = 1..6$	Read/Write	Displays security group distinguished name. Used with the schema-free directory configuration only.
oemhp_group{n}_priv where $n = 1..6$	Read/Write	Assigns privileges to a group. Use a comma-separated list of the following: <ul style="list-style-type: none"> 1 (Administer Group Accounts) 2 (Remote Console Access) 3 (Virtual Power & Reset) 4 (Virtual Media) 5 (Configure iLO 2 Settings) Used with the schema-free directory configuration only.

Examples

- `set /map1/oemhp_dircfg1`

- `set /map1/oemhp_dircfg1 oemhp_dirauth=default_schema oemhp_dirsrvaddr=adserv.demo.com`

You can define additional groups using additional set commands.

You can specify one or more properties on the command line. If there are multiple properties on the same command line, they must be separated by a space.

Virtual media commands

Access to the iLO 2 virtual media is supported through the CLP. The virtual media subsystem is located at `/map1/oemhp_vm1`. See the user guide for more information.

Targets

You can access the following sub-components of the virtual media.

Target	Description
<code>/map1/oemhp_vm1/floppydr1</code>	Virtual floppy or key drive device
<code>/map1/oemhp_vm1/cddr1</code>	Virtual CD-ROM device

Properties

Property	Access	Description
<code>oemhp_image</code>	Read/Write	The image path and name for virtual media access. The value is a URL with a maximum length of 80 characters.
<code>oemhp_connect</code>	Read	Displays if a virtual media device is already connected through the CLP or scriptable virtual media.
<code>oemhp_boot</code>	Read/Write	Sets the boot flag. The valid values are: <ul style="list-style-type: none"> • Never—Do not boot from the device. The value is displayed as <code>No_Boot</code>. • Once—Boot from the device only once. The value is displayed as <code>Once</code>. • Always—Boot from the device each time the server is rebooted. The value is displayed as <code>Always</code>. • Connect—Connect the virtual media device. Sets <code>oemhp_connect</code> to <code>Yes</code> and <code>oemhp_boot</code> to <code>Always</code>. • Disconnect—Disconnects the virtual media device and sets the <code>oemhp_boot</code> to <code>No_Boot</code>.
<code>oemhp_wp</code>	Read/Write	Enables or disables the write-protect flag. Boolean values accepted.
<code>oemhp_applet_connected</code>	Read	Indicates if the Java™ applet is connected.

Image URL

The `oemhp_image` value is a URL. The URL, which is limited to 80 characters, specifies the location of the virtual media image file on an HTTP server and is in the same format as the scriptable virtual media image location.

URL example:

protocol://username:password@hostname:port/filename

- The protocol field is mandatory and must be either HTTP or HTTPS.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional.
- The filename field is mandatory.

The CLP performs only a cursory syntax verification of the <URL> value. You must visually verify the URL is valid.

Examples

- `set oemhp_image=http://imgserver.company.com/image/dosboot.bin`
- `set oemhp_image=http://john:abc123@imgserver.company.com/VMimage/install11Disk.iso`

iLO 1.60 CLI support

The `vm` simple CLI commands are still supported for virtual media:

- `vm device insert path`—Inserts an image
- `vm device eject`—Ejects an image
- `vm device get`—Gets the status of the virtual media
- `vm device set boot access`—Sets the status of the virtual media

Command options:

- Valid device names are `floppy` or `cdrom`

NOTE: USB key drives must be used with the `floppy` keyword syntax.

- The path is the URL to the media image
- Boot options are `boot_once`, `boot_always`, `no_boot`, `connect`, or `disconnect`
- Access options are `write_protect` or `write_allow`.

For more information about how to use these commands, see the commands `INSERT_VIRTUAL_MEDIA`, `EJECT_VIRTUAL_MEDIA`, `GET_VM_STATUS`, and `SET_VM_STATUS` in the section "Using RIBCL (on page 70)."

Tasks

- Insert a floppy USB key image into the Virtual Floppy/USBKey:
`cd /map1/oemhp_vm1/floppydr1`
`show`
`set oemhp_image=http://my.imageserver.com/floppyimg.bin`
`set oemhp_boot=connect`
`show`

This example executes the following commands:

- Change the current context to the floppy or key drive.
- Show the current status to verify that the media is not in use.
- Insert the desired image into the drive.

- Connect the media. The boot setting always connects automatically.
- Eject a floppy or USB key image from the Virtual Floppy/USBKey:

```
cd /map1/oemhp_vm1/floppydr1
set oemhp_boot=disconnect
```

This example executes the following commands:

 - Change the current context to the floppy or key drive.
 - Issue the disconnect command that disconnects the media and clears the oemhp_image.
- Insert a CDROM image into the virtual CD-ROM:

```
cd /map1/oemhp_vm1/cddr1
show
set oemhp_image=http://my.imageserver.com/ISO/install_disk1.iso
set oemhp_boot=connect
show
```

This example executes the following commands:

 - Change the current context to the CD-ROM drive.
 - Show the current status to verify that the media is not in use.
 - Insert the desired image into the drive.
 - Connect the media. The boot setting always connects automatically.
- Eject a CD-ROM image from the Virtual CD-ROM:

```
cd /map1/oemhp_vm1/cddr1
set oemhp_boot=disconnect
```

This example executes the following commands:

 - Change the current context to the CD-ROM drive.
 - Issue the disconnect command that disconnects the media and clears the oemhp_image.
- Insert a CD-ROM image and set for single boot:

```
cd /map1/oemhp_vm1/cddr1
set oemhp_image=http://my.imageserver.com/ISO/install_disk1.iso
set oemhp_boot=connect
set oemhp_boot=once
show
```

This example executes the following commands:

 - Change the current context to the CD-ROM drive.
 - Show the current status to verify that the media is not in use.
 - Insert the desired image into the drive.
 - Connect the media. The boot setting always connects automatically.
 - Override the boot setting to Once.
- Eject a CD-ROM image from the virtual CD-ROM in a single command:

```
set /map1/oemhp_vm1/cddr1 oemhp_boot=disconnect
```

If you attempt to disconnect when the drive is not connected, you receive an error.

Start and reset commands

Start and reset commands enable you to power on and reboot the server containing iLO 2 or the iLO 2 itself.

Command	Description
start	Turns server power on
stop	Turns server power off
reset hard	Power cycles the server
reset soft	Warm boots the server

Examples

If the current target is `/system1`, the following commands are supported:

- `start`
- `stop`
- `reset hard`
- `reset soft`

If the current target is `/map1`, the following commands are supported:

- `reset`
- `reset soft`

iLO 1.60 CLI support

- **power**

The power command is used to change the power state of the server and is limited to users with the Power and Reset privilege.

- `power`—Displays the current server power state
- `power on`—Turns the server on
- `power off`—Turns the server off
- `power reset`—Resets the server (server power off followed by server power on)
- `power warm`—Warm boots the server

Instead of using the simple commands, the following examples show the new CLP format:

- `start /system1`—Turns the server on
- `stop /system1`—Turns the server off
- `reset /system1`—Resets the server
- `reset /system1 hard`—Performs a coldstart reboot of the server
- `reset /system1 soft`—Performs a warmstart reboot of the server
- `show /system1 enabledstate`—Shows the current power state, for which enabled is powered on and disabled is powered off.

- **vsp**

The vsp command invokes a virtual serial port session. When in virtual serial port session, press `Esc (` to return to the CLI.

Instead of using the simple commands, the following example shows the new CLP format:

```
start /system1/oemhp vsp1
```

- **remcons**

The `remcons` command starts a Remote Console session and is limited to users with the Remote Console privilege. Only a text-based remote console is supported, similar to a telnet session. When in Remote Console session, enter `Esc (` to return to the CLI.

Instead of using the simple commands, the following example shows the new CLP format:

```
start /system1/console1
```

Firmware update

Firmware commands enable you to display and modify the iLO 2 firmware version. Firmware settings are available at `/map1/firmware`.

Targets

No targets

Properties

Property	Access	Description
version	read	Displays the current firmware version.
date	read	Displays the release date of the current firmware version.

Command format

```
load -source <URL> [<target>]
```

where `<URL>` is the URL of firmware update image file on web server. The URL is limited to 50 characters in the iLO 1.70 release of the firmware.

URL example:

```
protocol://username:password@hostname:port/filename
```

- The protocol field is mandatory and must be either HTTP or HTTPS.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional
- The filename field is mandatory.

The CLP only performs a cursory syntax verification of the `<URL>` value. You must visually ensure the URL is valid.

Examples

```
load -source http://imgserver.company.com/firmware/iloFWimage.bin
load -source http://john:abc123@imgserver.company.com/firmware/ilo.bin
```

The `[<target>]` field is `/map1/firmware`, and is optional if it is already the default target.

Eventlog commands

Eventlog commands enable you to display or delete the logs of both the system and iLO 2. Eventlog settings are available at:

- `/system1/log1` for the system event log
- `/map1/log1` for the iLO 2 event log

Targets

record:1..n, where n is the total number of records

Properties

Property	Access	Description
number	read	Displays the record number for the event.
severity	read	Displays the severity of the event. It can be informational, noncritical, critical, or unknown.
date	read	Displays the event date.
time	read	Displays the event time.
description	read	Displays a description of the event.

Examples

- `show /system1/log1`—Displays system event log.
- `show /map1/log1`—Displays the iLO 2 event log.
- `show /system1/log1/recordn`—Displays record n from the system event default text.
- `show /map1/log1/recordn`—Displays record n from the iLO 2 event log.
- `delete /system1/log1`—Deletes system event log.
- `delete /map1/log1`—Deletes iLO 2 event log.

Blade commands

Blade commands enable you to view and modify the values on a p-Class server. These values are available at `/system1/map1/blade1`.

Targets

You can access the following subcomponents of the blade:

Target	Description
<code>/map1/blade1/diagport</code>	Displays and modifies the front diagnostic port settings.
<code>/map1/blade1/rack</code>	Displays and modifies the blade rack settings.
<code>/map1/blade1/rack1/enclosure1</code>	Displays and modifies the blade enclosure settings.

Properties

Property	Access	Description
bay_name	Read	Displays and modifies the blade bay name.
bay_number	Read	Displays the blade bay number.
facility_power	Read	Displays and modifies if the blade 48 V power is provided by the facility.
auto_power	Read	Displays and modifies if the blade is enabled to automatically power up.

Property	Access	Description
log_alerts	Read/write	Displays and modifies if rack alert logging is enabled.
autoselect	Read/write	Displays and modifies the diagnostic port autoselect setting.
speed	Read/write	Displays and modifies the diagnostic port speed setting.
fullduplex	Read/write	Displays and modifies if the diagnostic port supports full-duplex or half-duplex mode.
ipaddress	Read/write	Displays and modifies the IP address for the diagnostic port.
mask	Read/write	Displays and modifies the subnet mask for the diagnostic port.
rack_name	Read/write	Displays and modifies the rack name.
rack_sn	Read	Displays the rack serial number.
encl_name	Read/write	Displays and modifies the enclosure name.
ser	Read	Displays the enclosure serial number.
encl_type	Read	Displays the enclosure type.

Examples

- `set /map1/blade1/bay_name=BayOne`—Sets the blade bay name to BayOne.
- `show /map1/blade1/diagport1/ipaddress`—Displays the IP address of the front diagnostic port.
- `show /map1/blade1/rack1/enclosure1 (N) /encl_type`—Displays the enclosure type for blade enclosure *N*.

Boot commands

Boot commands enable you to modify the boot source and boot order of the system. Boot settings are available at `/system1/bootconfig1`.

Targets

`bootsource1..n`, where *n* is the total number of boot sources

Sets the boot source for the system. The possible values are:

- `BootFmCd : bootsource1`
 - `BootFmFloppy : bootsource2`
 - `BootFmDrive : bootsource3`
 - `BootFmNetwork : bootsource4`
- or
- `BootFmCd : bootsource1`
 - `BootFmFloppy : bootsource2`

- `BootFmDrive : bootsource3`
- `BootFmUSBKey : bootsource4`
- `BootFmNetwork : bootsource5`

Properties

Property	Access	Description
<code>bootorder</code>	Read/write	Sets the boot order for a given boot source

Examples

- `set /system1/bootconfig1/bootsource(n) bootorder=(num)`
- `show /system/bootconfig1`—Displays the complete boot configuration
- `show /system1/bootconfig1/bootsource1`—Displays `bootorder` for `bootsource1`

LED commands

LED commands are used to change the state of the UID light on the server. LED settings are available at `/system1/led1`.

Property	Description
<code>start</code>	Turns the LED on.
<code>stop</code>	Turns the LED off.
<code>show</code>	Displays the LED status.

Examples

- `show /system1/led1`—Displays current LED status
- `start /system1/led1`—Turns LED on
- `stop /system1/led1`—Turns LED off

iLO 1.60 CLI support

Simple UID CLI commands introduced in iLO 1.60 are still supported.

- `uid`—Displays the current UID state on the server.
- `uid on`—Turns the UID light on.
- `uid off`—Turns the UID light off.

Instead of using the simple commands, the following examples show the new CLP format:

- `show /system1/led1`—verifies LED status
- `start /system1/led1`—Turns LED on
- `stop /system1/led1`—Turns LED off

System properties and targets

The properties and targets, described in this section, provide information about the server.

Targets

Target	Description
oemhp_PresentPower	Displays the average power reading from the last sample.
oemhp_AveragePower	Displays the average power reading from the past 24 hours.
oemhp_MaxPower	Displays the greatest peak power reading from the past 24 hours.
oemhp_MinPower	Displays the minimum average power reading from the past 24 hours.
warning_type	Displays and modifies the warning type.
warning_threshold	Displays and modifies the warning threshold for power consumption.
warning_duration	Displays and modifies the duration the power threshold must be exceeded before a warning is generated.

The following properties are available in /system1.

Property	Access	Description
name	Read	Displays the system name.
number	Read	Displays the system serial number.
oemhp_server_name	Read	Displays the host server name string. This string can be up to 50 characters in length, and requires the configure iLO 2 privilege to change.
enabledstate	Read	Appears if the server is powered up.
oemhp_powerreg	Read/write	Displays the setting for dynamic power saver mode. Valid values are dynamic, min, max, and os.
processor_number	Read	Displays the number of logical processors in the system.
pstate_number	Read	Displays the number of p-states supported by the server.
oemhp_pwracap	Read/write	Displays the current power cap of the server. The value is shown in watts. You cannot set this property when a dynamic power cap is set for the Enclosure. Enclosure Dynamic Power Caps is set and modified using either Onboard Administrator or Insight Power Manager.
oemhp_power_micro_ver	Read	Displays the version and current state of the power micro option.

Examples

- `show /system1`
- `show /system1 name`
- `set /system1 oemhp_powergov=auto`

The `cpu` property is a target of `/system1` and displays information about the system processor. The following properties are available in `/system1/cpu<n>`:

Property	Access	Description
speed	Read	Displays the processor speed.
cachememory1	Read	Displays the size of the processor level-1 cache.
cachememory2	Read	Displays the size of the processor level-2 cache.
logical_processor<n>	Read	Displays the logical processor.

CPU power state—Enables you to examine the CPU power states. CPU power state values are shown as a part of the `cpu` target and use an additional property of `logical_processor<n>`.

Example:

The `show cpu1/logical_processor1` command displays the p-states of the processor: For example:
`/system1/cpu1/logical_processor1`

Targets

Properties

```
current_pstate=1
pstate0_avg=0.0
pstate1_avg=100.0
pstate2_avg=0.0
pstate3_avg=0.0
pstate4_avg=0.0
pstate5_avg=0.0
pstate6_avg=0.0
pstate7_avg=0.0
```

Memory—Displays information about the system memory.

The following properties are available in `/system1/memory<n>`:

Property	Access	Description
size	Read	Displays the memory size.
speed	Read	Displays the memory speed.
location	Read	Displays the location of the memory.

Slot—Displays information about the system slots.

The following properties are available in `/system1/slot<n>`:

Property	Access	Description
type	Read	Displays the slot type.

Property	Access	Description
width	Read	Displays the slot width.

Firmware—Displays information about the system ROM.

The following properties are available in `/system1/firmware`:

Property	Access	Description
version	Read	Displays the version of the system ROM.
date	Read	Displays the date the system ROM.

Examples:

- `show /system1/cpu1` displays information on one CPU.
- `show /system1/memory1` displays information on one memory slot.
- `show /system1/slot1` displays information on one slot.
- `show /system1/firmware1` displays information about system ROM. For example:
`/system1/firmware1`

Targets

Properties

version=P56

date=01/05/2006

NOTE: `system1/cpu`, `system1/memory`, and `system1/slot` are not supported in iLO 1.81.

Other commands

- `start /system1/oemhp vsp1`—Starts virtual serial port session. Press `ESC (` to revert back to the CLI session.
- `nmi server`—Generates and sends an NMI to the server and is limited to users with the Power and Reset privilege.

Telnet

Telnet support

iLO 2 supports the use of telnet to access the iLO 2 command line interface. Telnet access to iLO 2 supports the CLI, which can invoke a Remote Console connection as well as a Virtual Serial Port connection. Refer to the "Command line (on page 10)" section for more information.

Using Telnet

To use telnet, the iLO 2 Remote Console Port Configuration and Remote Console Data Encryption on the Global Settings screen must be configured as follows:

1. Set the Remote Console Port Configuration to **Enabled**.
2. Set the Remote Console Data Encryption to **No**.

You can open either a telnet based Remote Console session or a browser-based Remote Console session. You cannot open both at the same time. An error message is generated if both sessions are opened simultaneously.

To access iLO 2 using telnet:

1. Open a telnet window.
2. When prompted, enter the IP address or DNS name, login name, and password.

NOTE: Access through telnet will be disabled, if the remote console port configuration on the Global Settings tab is set to Disabled or Automatic, or if remote console data encryption is enabled.

To terminate a telnet session:

1. Press the **Ctrl+] keys** and press the **Enter** key at the prompt.
2. If you see an extra carriage return each time the Enter key is pressed, press the **Ctrl+] keys** and enter `set crlf off` at the prompt.

Refer to "iLO 2 VT100+ Key Map (on page 37)" for a complete list of key sequences.

Telnet simple command set

The following key sequences for simple command set are available for use during telnet sessions. These commands are available only when in a telnet-based Remote Console or Virtual Serial Port session.

Action	Key sequence	Comment
POWER ON	CTRL P 1	CTRL P is the prefix for the Power commands. The 1 indicates an ON selection.

Action	Key sequence	Comment
POWER OFF	CTRL P 0	CTRL P is the prefix for the Power commands. The 0 indicates an OFF selection.
ACPI PRESS	CTRL P 6	CTRL P is the prefix for the Power commands. The 6 indicates an ACPI power press. The ACPI power press is equivalent to holding the power button for approximately 6 seconds.
SYSTEM REBOOT	CTRL P !	CTRL P is the prefix for the Power commands. The ! indicates an immediate emergency reboot.
UID ON	CTRL U 1	CTRL U is the prefix for the UID commands. The 1 indicates an ON selection.
UID OFF	CTRL U 0	CTRL U is the prefix for the UID commands. The 0 indicates an OFF selection.

The keys do not work before authentication. The power control requests are correctly ignored when you do not have the correct power control privileges.

Telnet security

Telnet is an unsecured network protocol. To reduce any security risks:

- Use SSH instead of telnet. SSH is essentially secure or encrypted telnet. CLI is supported through telnet as well as SSH.
- Use a segregated management network. Preventing unauthorized access to the network segment prevents unauthorized activity.

Supported key sequences

iLO 2 supports the VT100+ protocol. The following tables define the supported key sequences.

iLO 2 VT100+ key map

The following are VT100+ key sequences.

- Many terminal programs send CR-LF when they mean ENTER.
Sequence `"\r\n"` = `'\r'`
- Some terminals send ASCII 127 (DEL) when they mean backspace. The Delete key never sends DEL. It sends `"\e[3~"`.
- Some programs use the following mapping for HOME and END:
sequence `"\e[H"` = HOME_KEY
sequence `"\e[F"` = END_KEY
- ALT_CAPITAL_O and ALT_LEFT_SQBRACKET are ambiguous.

- Terminate longer sequences that start with \eO and \e[, with \?.

Key	Sequence	Key	Sequence
\010	\177	ALT_AMPER	\e&
UP_KEY	\e[A	ALT_APOS	\e'
DOWN_KEY	\e[B	ALT_OPAREN	\e(
RIGHT_KEY	\e[C	ALT_CPAREN	\e)
LEFT_KEY	\e[D	ALT_STAR	\e*
ALT_A	\eA	ALT_PLUS	\e+
ALT_B	\eB	ALT_COMMA	\e,
ALT_C	\eC	ALT_MINUS	\e-
ALT_D	\eD	ALT_PERIOD	\e.
ALT_E	\eE	ALT_SLASH	\e/
ALT_F	\eF	ALT_COLON	\e:
ALT_G	\eG	ALT_SEMICO	\e;
ALT_H	\eH	ALT_LESS	\e<
ALT_I	\eI	ALT_EQUAL	\e=
ALT_J	\eJ	ALT_MORE	\e>
ALT_K	\eK	ALT_QUES	\e?
ALT_L	\eL	ALT_AT	\e@
ALT_M	\eM	ALT_OPENSQ	\e[\?
ALT_N	\eN	ALT_BSLASH	\e\\
ALT_O	\eO\?	ALT_CLOSESQ	\e]
ALT_P	\eP	ALT_CARAT	\e^
ALT_Q	\eQ	ALT_USCORE	\e_
ALT_R	\eR	ALT_ACCENT	\e`
ALT_T	\eT	ALT_PIPE	\e
ALT_U	\eU	ALT_CBRACK	\e}
ALT_V	\eV	ALT_TILDE	\e~
ALT_W	\eW	ALT_TAB	\e\t
ALT_X	\eX	ALT_BS	\e\010
ALT_Y	\eY	ALT_CR	\e\r
ALT_Z	\eZ	ALT_ESC	\e\e\?
ALT_LOWER_A	\ea	ALT_F1	\e\eOP
ALT_LOWER_B	\eb	ALT_F2	\e\eOQ
ALT_LOWER_C	\ec	ALT_F3	\e\eOR

Key	Sequence	Key	Sequence
ALT_LOWER_D	\ed	ALT_F4	\e\eOS
ALT_LOWER_E	\ee	ALT_F5	\e\eOT
ALT_LOWER_F	\ef	ALT_F6	\e\eOU
ALT_LOWER_G	\eg	ALT_F7	\e\eOV
ALT_LOWER_H	\eh	ALT_F8	\e\eOW
ALT_LOWER_I	\ei	ALT_F9	\e\eOX
ALT_LOWER_J	\ej	ALT_F10	\e\eOY
ALT_LOWER_K	\ek	ALT_F11	\e\eOZ
ALT_LOWER_L	\el	ALT_F12	\e\eO[
ALT_LOWER_M	\em	ALT_F5	\e\e[15~
ALT_LOWER_N	\en	ALT_F6	\e\e[17~
ALT_LOWER_O	\eo	ALT_F7	\e\e[18~
ALT_LOWER_P	\ep	ALT_F8	\e\e[19~
ALT_LOWER_Q	\eq	ALT_F9	\e\e[20~
ALT_LOWER_R	\er	ALT_F10	\e\e[21~
ALT_LOWER_S	\es	ALT_F11	\e\e[23~
ALT_LOWER_T	\et	ALT_F12	\e\e[24~
ALT_LOWER_U	\eu	ALT_HOME	\e\e[1~
ALT_LOWER_V	\ev	ALT_INS	\e\e[2~
ALT_LOWER_W	\ew	ALT_DEL	\e\e[3~
ALT_LOWER_X	\ex	ALT_END	\e\e[4~
ALT_LOWER_Y	\ey	ALT_PGUP	\e\e[5~
ALT_LOWER_Z	\ez	ALT_PGDN	\e\e[6~
ALT_SPACE	\e\040	ALT_HOME	\e\e[H
ALT_EXCL	\e!	ALT_END	\e\e[F
ALT_QUOTE	\e\"	ALT_UP	\e\e[A
ALT_POUND	\e#	ALT_DOWN	\e\e[B
ALT_DOLLAR	\e\$	ALT_RIGHT	\e\e[C
ALT_PERCENT	\e%	ALT_LEFT	\e\e[D

VT100+ codes for the F-keys

Key	Sequence
F1_KEY	\eOP
F2_KEY	\eOQ
F3_KEY	\eOR
F4_KEY	\eOS
F5_KEY	\eOT
F6_KEY	\eOU
F7_KEY	\eOV
F8_KEY	\eOW
F9_KEY	\eOX
F10_KEY	\eOY
F11_KEY	eOZ
F12_KEY	\eO[

Linux codes for the F-keys

Key	Sequence
F5_KEY	\e[15~
F6_KEY	\e[17~
F7_KEY	\e[18~
F8_KEY	\e[19~
F9_KEY	\e[20~
F10_KEY	\e[21~
F11_KEY	\e[23~
F12_KEY	\e[24~
HOME_KEY	\e[1~
INSERT_KEY	\e[2~
DELETE_KEY	\e[3~
END_KEY	\e[4~
PG_UP	\e[5~
PG_DOWN	\e[6~

Secure Shell

SSH overview

SSH is a telnet-like program for logging into and for executing commands on a remote machine, which includes security with authentication, encryption, and data integrity features. iLO 2 can support simultaneous access from two SSH clients. After SSH is connected and authenticated, the command line interface is available.

iLO 2 supports:

- SSH protocol version 2
- PuTTY 0.54, which is a free version of telnet and SSH protocol available for download on the Internet. When using PuTTY, versions before 0.54 might display 2 line feeds instead on a single line feed, when the ENTER key is pressed. To avoid this issue and for best results, HP recommends using version 0.54 or later.
- OpenSSH, which is a free version of the SSH protocol available for download on the Internet.

When upgrading the firmware, there is a one-time 25-minute delay before SSH functionality is available. During this time, iLO 2 generates the 1024-bit RSA and DSA keys. These keys are saved by iLO 2 for future use. If iLO 2 is reset to factory defaults, the RSA and DSA keys are erased and are regenerated on the next boot.

SSH features supported by iLO 2

The iLO 2 library supports only version 2 (SSH-2) of the protocol. The features that are supported are listed in the following table.

Feature	Supported algorithm
Server host key algorithms	ssh-dss , ssh-rsa
Encryption (same set supported both ways)	3des-cbc, aes128-cbc
Hashing algorithms	hmac-sha1, hmac-md5
Public key algorithms	ssh-dss, ssh-rsa
Key exchange	Diffie-hellman-group1-sha1
Compression	None
Language	English
Client/User authentication method	Password
Authentication timeout	2 minutes
Authentication attempts	3
Default SSH port	22

Using Secure Shell

Using SSH

To access iLO 2 using SSH:

1. Open an SSH window.
2. When prompted, enter the IP address or DNS name, login name, and password.

Using OpenSSH

To start an OpenSSH client in Linux, use:

```
ssh -l loginname ipaddress/dns name
```

Using PuTTY

- To start a PuTTY session, double-click the PuTTY icon in directory where PuTTY is installed.
- To Start a PuTTY session from the command line:
 - To start a connection to a server called *host*:

```
putty.exe [-ssh | -telnet | -rlogin | -raw] [user@]host
```
 - For telnet sessions, the following alternative syntax is supported:

```
putty.exe telnet://host[:port]/
```
 - To start an existing saved session called *sessionname*:

```
putty.exe -load "session name"
```

SSH key authorization

SSH key-based authentication enables HP SIM to connect to LOM devices through SSH and be authenticated and authorized to perform administrative-level tasks. The CLP is utilized to perform tasks. HP SIM can perform these tasks on multiple LOM devices nearly simultaneously, at scheduled times. HP SIM provides a menu-driven interface to manage and configure multiple targets. Enhancements to HP SIM are provided by tool definition files.

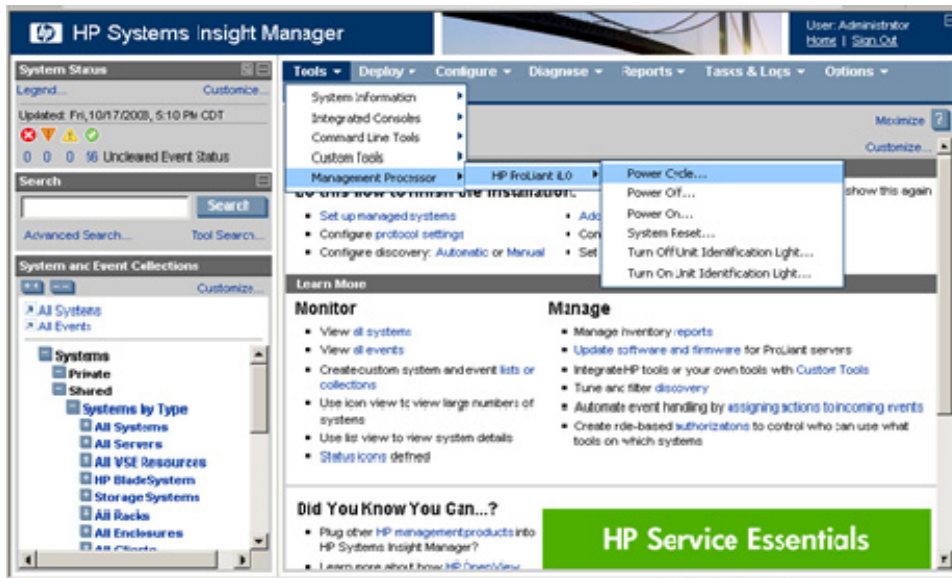
HP SIM can perform actions on target devices utilizing an SSH interface that requires private key-based authentication. If HP SIM is enabled to integrate more fully with LOM devices, SSH key-based authentication is implemented in iLO 2.

An HP SIM instance will be established as a trusted SSH client by installing its public key in iLO 2. This is completed either manually through a Web-based GUI, or automatically with the `mxagentconfig` utility.

SSH keys do not need to be created to use SSH in interactive mode. To use SSH in interactive mode, see the "SSH overview (on page 41)" section.

Tool definition files

TDEF files extend the menu system of HP SIM to provide the CLP commands that HPSIM transmits to iLO 2 through an SSH connection.



Mxagentconfig

Mxagentconfig is a utility used to export and install HP SIM public SSH keys into other systems. This utility simplifies the process and can install the public key on many systems simultaneously. Mxagentconfig will make an SSH connection to iLO 2, authenticate with a user name and password, and transmit the necessary public key. iLO 2 stores this key as a trusted SSH client key.

Importing SSH keys from PuTTY

The public key file format generated by PuTTY is not compatible with iLO 2. The following example illustrates, a PuTTY generated public key file:

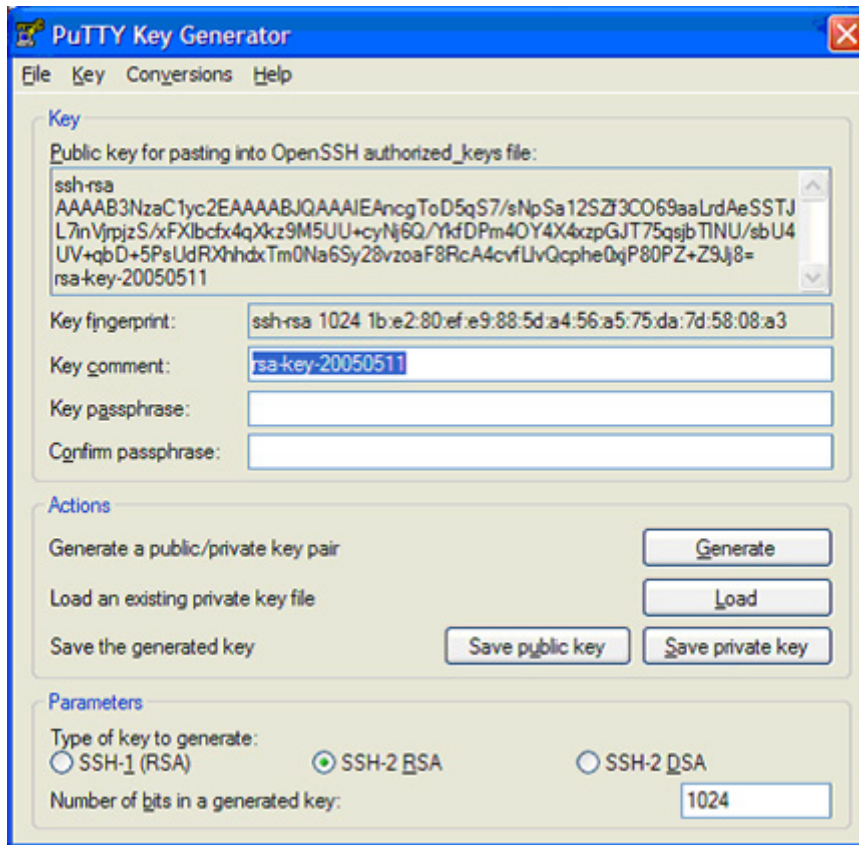
```
----- BEGIN SSH2 PUBLIC KEY -----
Comment: "Administrator"
AAAAB3NzaC1yc2EAAAABJQAAAIB0x0wVO9itQB11o+tHnY3VvmsGgwghCyLOVzJl
3A9F5yzKj+RXJVPxOGusAhmJwF8PBQ9wV5E0Rumm6gNOaPyvAMJCG/10PW7Fhac1
VLt8i5F3Loss+/LWa+6H0da13TF2vq3ZoYFUT4esC6YbAACM7kLuGwxF5XMNR2E
Foup3w==
----- END SSH2 PUBLIC KEY -----
```

iLO 2 expects public key file information on a single line. You must use the PuTTY Key Generator (puttygen.exe) utility to import a correctly formatted SSH key for use with iLO 2.

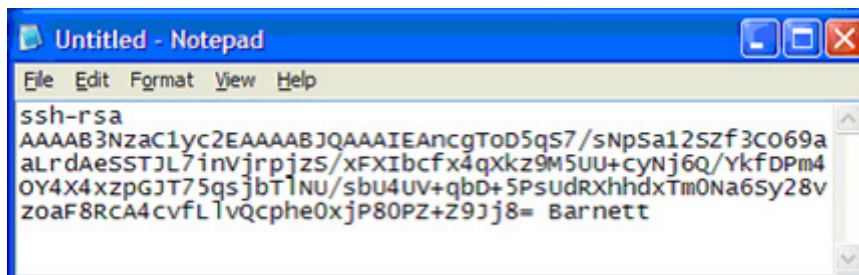
To import SSH keys to iLO 2 from PuTTY:

1. Double-click the PuTTY Key Generator icon to launch the utility.
2. Select **SSH-2 RSA**, and then click **Generate**.

On the key area, move the mouse around to generate the key. You must keep moving the mouse until the key generation process is complete.

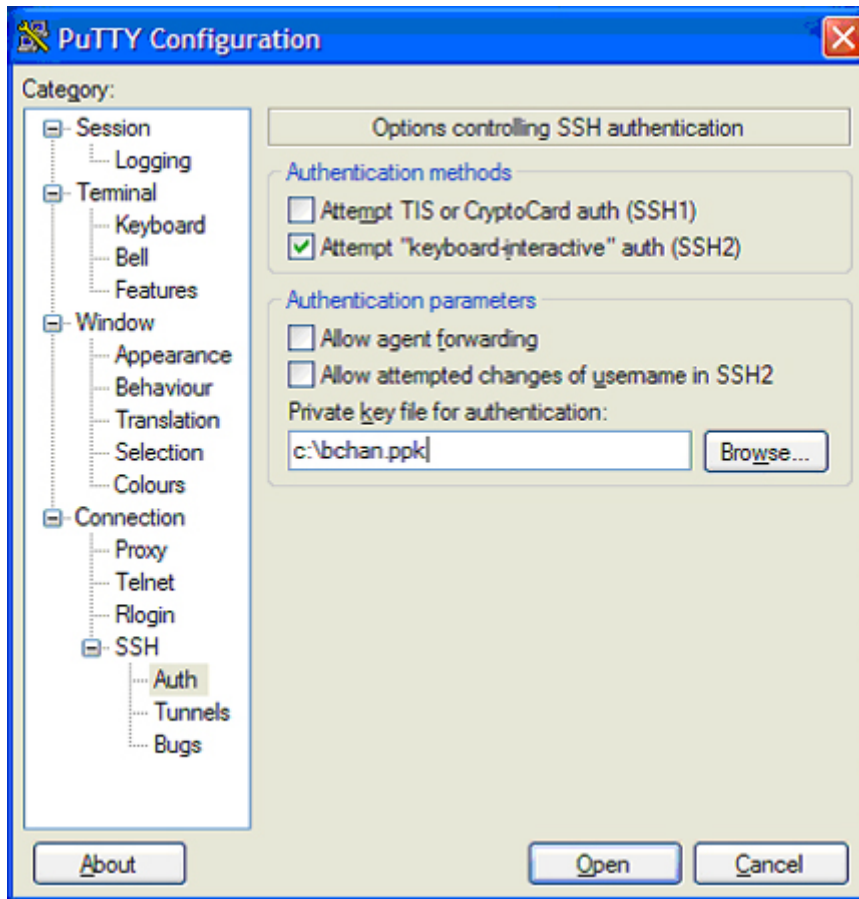


3. After the key is generated, replace the key comment with your iLO 2 user name. (The user name is case-sensitive.)
4. Select all the text in the public key area. Copy the key and paste it into a Notepad session.
5. Return to the PuTTY Key Generator utility.
6. Click **Save private key** to save, and then enter a file name when prompted, for example, c:\bchan.ppk.
7. Return to Notepad.
8. Save the public key file. Click **File>Save As**, and then enter a file name when prompted, for example, c:\bchan.pub.



9. Log into iLO 2 (if not already open).
10. On the iLO 2 SSH Key Administration page, click **Browse**, and then locate the public key file.
11. Click **Authorize Key**. A new Authorized SSH key appears in the list.
12. Launch PuTTY.

13. Select **SSH>Auth**.
14. Click **Browse**, and locate the private key file.
15. Configure your iLO 2 IP, and then click **Open**. iLO 2 prompts for a user name.



16. Enter the logon name associated with the public key. The public key in iLO 2 authenticates with the private key in PuTTY. If the keys match, you are logged into iLO 2 without using a password.
Keys can be created with a key passphrase. If a key passphrase was used to generate the public key, you are prompted for the key passphrase before you log into iLO 2.

Importing SSH keys generated using ssh-keygen

After generating an SSH key using ssh-keygen and creating the key.pub file, you must do the following:

1. Locate and open the key.pub file with a text editor. The file should begin with the text `ssh-dss` or `ssh-rsa`.
2. At the end of the line, append a " " (space) and the name of a valid iLO 2 user name as shown on the Modify User page. For example: `xxx_some text_xxx ASmith`

The user name is case-sensitive and must match the case of the iLO 2 user name to associate the SSH key with the correct user.

3. Save and close the file.

The key file is ready to import and authorize.

Group administration and iLO 2 scripting

Lights-Out Configuration Utility

The Lights-Out Configuration Utility (CPQLOCFG.EXE) is a Microsoft® Windows®-based utility that connects to the iLO 2 using a secure connection over the network. RIBCL scripts are passed to the iLO 2 over the secure connection to CPQLOCFG. This utility requires a valid user ID and password with the appropriate privileges. The CPQLOCFG utility can be launched from HP SIM for Group Administration or used independently from a command prompt for batch processing. This utility can be downloaded from the HP website (<http://h18004.www1.hp.com/support/files/lights-out/us/index.html>).

Version 2.27 or later of CPQLOCFG.EXE is required to support all features of iLO 1.93 and later and iLO 2 1.00 and later.

HP SIM discovers iLO 2 devices as management processors. The Lights-Out Configuration Utility sends a RIBCL file to a group of iLO 2s to manage the user accounts for those iLO 2 devices. The iLO 2 devices then perform the action designated by the RIBCL file and send a response to the log file.

The Lights-Out Configuration Utility is used to execute RIBCL scripts on the iLO 2 and must reside on the same server as HP SIM. The Lights-Out Configuration Utility generates two types of error messages: runtime and syntax.

- Runtime errors occur when an invalid action is requested. Runtime errors are logged to the C:\PROGRAM FILES\INSIGHT MANAGER\HP\SYSTEMS directory.
- Syntax errors occur when an invalid XML tag is encountered. When a syntax error occurs, the Lights-Out Configuration Utility stops running and logs the error in the runtime script and output log file.

Syntax errors take the format of Syntax error: expected X but found Y. For example:

Syntax error: expected USER_LOGIN=userlogin but found USER_NAME=username.

For a complete listing of errors, see "Using RIBCL (on page 70)."

Unauthenticated XML query

If configured to do so, the iLO 2 device will return some identifying information in response to an unauthenticated XML query. By default, the iLO 2 is configured to return this information. To disable this feature, set the CIM_SECURITY_MASK in the MOD_SNMP_IM_SETTINGS command to disallow returned information.

To obtain unauthenticated identifying information, submit the following command to the iLO 2 web server port:

```
https://<ioloadress>/xmldata?item=all
```

A typical response to this command is:

```
<?xml version="1.0" ?>
<RIMP>
  <HSI>
    <SBSN>0004PBM158</SBSN>
```

```

        <SPN>ProLiant DL380 G5</SPN>
        <UUID>1226570004PBM158</UUID>
        <SP>1</SP>
    </HSI>
    <MP>
        <ST>1</ST>
        <PN>Integrated Lights-Out 2 (iLO 2)</PN>
        <FWRI>1.10</FWRI>
        <HWRI>ASIC: 5</HWRI>
        <SN>ILO0004PBM158</SN>
        <UUID>ILO1226570004PBM158</UUID>
    </MP>
</RIMP>

```

Query definition in HP SIM

To group all of the iLO 2 devices, log in to HP SIM and create a query.

To create the query:

1. Log in to HP SIM.
2. Click **Device** in the navigation bar on the top left side of the screen.
3. Click **Queries>Device**.
4. Locate the Personal Queries section in the main window. If a query category exists, proceed to step 7, otherwise proceed to step 5.
5. Click **New** to create a new category. For this example, the name of the new category is RIB Cards. Click **Create Category**.
6. Click **Queries** to return to the Device Queries screen.
7. Click **New**, within the appropriate query category, to open the Create/Edit Query screen where the query definition is created.
8. Define the query name, for example "Mgmt Processors."
9. Select **Device(s) of type**, and then select **Devices by product name**. In the criteria windows, set the product name to **HP Integrated Lights-Out 2**.
10. Click **type** in the Query Description field. A window opens where you define the device type.
11. Select **Management Processor** and click **OK**.
12. Click **Save** to return to the Device Query screen.
13. Find the newly created query in the appropriate query category, and click the query name to run it for verification.
14. Click **Overview** on the left side of the screen after the verification has taken place. The initial page for devices opens.

Application Launch using HP SIM

The Application Launch combines the RIBCL, the Lights-Out Configuration Utility, and the query definition to manage the Group Administration of the iLO 2s.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the Tasks screen.
3. Click **New Control Task** and select **Application Launch** from the dropdown menu to open the Create/Edit Task screen.
4. Enter the full path and name for the Lights-Out Configuration Utility in the area provided. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
5. Enter the parameters in the area provided. HP SIM requires the following parameters for the Lights-Out Configuration Utility:

-F is the full path of the RIBCL file name.

-V is the verbose message (optional).

If the RIBCL file is in the root directory of on the C:\ drive, then the parameters are:

-F C:\MANAGEUSERS.xml -V

NOTE: The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

6. Click **Next**. A screen displays the options for naming the task, defining the query association, and setting a schedule for the task.
7. Enter a task name in the Enter a name for this task field.
8. Select the query that had been created earlier, for example "Mgmt Processors."
9. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window appears.
10. Click **OK** to set the schedule.

NOTE: The default schedule for a control task is **Now**.

11. Click **Finish** to save the Application Launch task.
12. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

Batch processing using the Lights-Out Configuration Utility

Group Administration can also be delivered to iLO 2 through batch processing. The components used by batch processing are the Lights-Out Configuration Utility, an RIBCL file, and a batch file.

The following example shows a sample batch file that can be used to perform the Group Administration for iLO 2:

```
REM Updating the HP Integrated Lights-Out 2 board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
```



```
RIBNLOG -S RIBN -F C:\...\SCRIPT.XML -L LOGFILE.TXT -V
```

The Lights-Out Configuration Utility overwrites any existing log files.

Lights-Out Configuration Utility parameters

- The **-S** switch is the switch that determines the iLO 2 that is to be updated. This switch is either the DNS name or IP address of the target server.
Do **not** use this switch if you are launching from HP SIM. HP SIM will provide the address of the iLO 2 when CPQLOCFG.EXE is launched.
- The **-F** switch is the switch that gives the full path location and name of the RIBCL file that contains the actions to be performed on the board.
- The **-U** and **-P** switches specify the user login name and password. These options allow the login information within the script file to be overridden.

Be sure that the Lights-Out Configuration Utility is in a directory referenced by the PATH environment variable. Any log files generated are placed in the same directory as the Lights-Out Configuration Utility executable

The **-L** and **-V** switches might or might not be set depending on the IT administrator's preferences.

- The **-L** switch defines where the log file generated and what the file name will be. If this switch is omitted, a default log file with the DNS name or the IP address is created in the same directory used to launch CPQLOCFG.

Do **not** use this switch if launching from HP SIM.

NOTE: The output values might need to be modified to match the RIBCL syntax.

NOTE: The **-L** parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

- The optional **-v** switch turns on the verbose message return. The resulting log file contains all commands sent to the Remote Insight board, all responses from the Remote Insight board, and any errors. By default, only errors and responses from GET commands are logged without this switch.
- The **-t namevaluepairs** switch substitutes variables (%variable%) in the input file with values specified in namevaluepairs. Separate multiple namevaluepairs with a comma (,).

For example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="%user%" PASSWORD="%password%">
    <USER_INFO MODE="read">
      <GET_ALL_USERS/>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

Using a command line enter:

```
Cpqlocfg -f filename -s serverip -t user=Admin,password=pass
```

If the parameter contains multiple words, you must enclose the phrase within double quotes (""). Up to 25 variables are supported in an XML file. The maximum length of variable name is 48 characters.

Web agent example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
  <MOD_SNMP_IM_SETTINGS>
    <WEB_AGENT_IP_ADDRESS value=%WebAgent%/>
  </MOD_SNMP_IM_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

Invoke the script using:

```
cpqlocfg -s <iLO-ip-name> -f mod_snmp_im_settings.xml -t
WebAgent='"Your_Value_Here"'
```

When replacing a token that requires double quotes, use single quotes around the token.

See "Using RIBCL (on page 70)" for information on the syntax of the XML data files. Sample XML scripts are available on the HP website (<http://www.hp.com/servers/lights-out>) in the Best Practices section.

Perl scripting

Using Perl with the XML scripting interface

The scripting interface provided enables administrators to manage virtually every aspect of the device in an automated fashion. Primarily, administrators use tools like the `cpqlocfg.exe` to assist deployment efforts. Administrators using a non-Windows® client can use Perl scripts to send XML scripts to the Lights-Out devices. Administrators can also use Perl to perform more complex tasks than `cpqlocfg.exe` can perform.

This section discusses how to use Perl scripting in conjunction with the Lights-Out XML scripting language. Perl scripts require a valid user ID and password with appropriate privileges. Sample XML scripts for Lights-Out devices and a sample Perl script are available on the HP website (<http://www.hp.com/servers/lights-out>) in the Best Practices section.

XML enhancements

Previous versions of iLO 2 firmware do not return properly formatted XML syntax. If the iLO 2 firmware determines the client utility does not support the return of properly formatted XML syntax, the following message appears:

```
<INFORM>Scripting utility should be updated to the latest
version.</INFORM>
```

This message informs you to update to a later version of the `cpqlocfg` scripting utility. The latest version of `cpqlocfg.exe` is 2.26.

If you are using a utility other than `cpqlocfg.exe` (such as Perl), the following steps might help ensure that the iLO 2 firmware returns properly formatted XML. You must incorporate `<LOCFG version="2.21">` into the script sent to iLO 2. You can place this tag in either the Perl script or the XML script. Placement of this tag is important. If you place this tag in the Perl script, the tag should be sent after `<?xml version="1.0"?>` and before the XML script is sent. If you place the tag in the XML script, the tag should be placed before `<RIBCL version="2.0">`. If you are using the Perl script provided by HP, you can add the bold line in the following example to return properly formatted XML syntax.

- Perl script modification

```
...
# Open the SSL connection and the input file
my $client = new IO::Socket::SSL->new(PeerAddr => $host);
open(F, "<$file") || die "Can't open $file\n";

# Send the XML header and begin processing the file
print $client '<?xml version="1.0"?>' . "\r\n";
#Send tag to iLO firmware to insure properly formatted XML is returned.
print $client '<LOCFG version="2.21">' . "\r\n";
...
```

- XML script modification

```

<!-- The bold line could be added for the return of properly formatted
XML. -->
<LOCFG version="2.21"/>
<RIBCL version="2.0">
    <LOGIN USER_LOGIN="Adminname" PASSWORD = "password">
        <!--
        Add XML script here.
        -->
    </LOGIN>
</RIBCL>
</LOCFG>

```

Opening an SSL connection

Perl scripts must open an SSL connection to the device's HTTPS port, by default port 443. For example:

```

use Socket;
use Net::SSLeay qw(die_now die_if_ssl_error);

Net::SSLeay::load_error_strings();
Net::SSLeay::SSLeay_add_ssl_algorithms();
Net::SSLeay::randomize();

#
# opens an ssl connection to port 443 of the passed host
#
sub openSSLconnection($)
{
    my $host = shift;
    my ($ctx, $ssl, $sin, $ip, $nip);

    if (not $ip = inet_aton($host))
    {
        print "$host is a DNS Name, performing lookup\n" if $debug;
        $ip = gethostbyname($host) or die "ERROR: Host $hostname not
        found.\n";
    }
    $nip = inet_ntoa($ip);
    print STDERR "Connecting to $nip:443\n";

    $sin = sockaddr_in(443, $ip);
    socket (S, &AF_INET, &SOCK_STREAM, 0) or die "ERROR: socket: $!";
    connect (S, $sin) or die "connect: $!";

    $ctx = Net::SSLeay::CTX_new() or die_now("ERROR: Failed to create
    SSL_CTX $! ");
    Net::SSLeay::CTX_set_options($ctx, &Net::SSLeay::OP_ALL);
    die_if_ssl_error("ERROR: ssl ctx set options");
    $ssl = Net::SSLeay::new($ctx) or die_now("ERROR: Failed to create SSL
    $!");
}

```

```

Net::SSLeay::set_fd($ssl, fileno(S));
Net::SSLeay::connect($ssl) and die_if_ssl_error("ERROR: ssl connect");
print STDERR 'SSL Connected ';
print 'Using Cipher: ' . Net::SSLeay::get_cipher($ssl) if $debug;
print STDERR "\n\n";

return $ssl;
}

```

Sending the XML header and script body

After the connection is established, the first line of script sent must be an XML document header, which tells the device's HTTPS web server that the following content is an XML script. The header must match the header used in the example exactly. After the header has been completely sent, the remainder of the script can be sent. In this example, the script is sent all at once. For example:

```

# usage: sendscript(host, script)
# sends the xmlscript script to host, returns reply
sub sendscript($$)
{
    my $host = shift;
    my $script = shift;
    my ($ssl, $reply, $lastreply, $res, $n);

    $ssl = openSSLconnection($host);

    # write header
    $n = Net::SSLeay::ssl_write_all($ssl, '<?xml version="1.0"?>'. "\r\n");
    rint "Wrote $n\n" if $debug;

    # write script
    $n = Net::SSLeay::ssl_write_all($ssl, $script);
    print "Wrote $n\n$script\n" if $debug;

    $reply = "";
    $lastreply = "";

    READLOOP:
    while(1)
    {
        $n++;
        $reply .= $lastreply;
        $lastreply = Net::SSLeay::read($ssl);
        die_if_ssl_error("ERROR: ssl read");
        if($lastreply eq "")
        {
            sleep(2); # wait 2 sec for more text.

```

```

        $lastreply = Net::SSLeay::read($ssl);
last READLOOP if($lastreply eq "");
    }
    sleep(2); # wait 2 sec for more text.
    $lastreply = Net::SSLeay::read($ssl);
    last READLOOP if($lastreply eq "");
    }
    print "READ: $lastreply\n" if $debug;
    if($lastreply =~ m/STATUS="(0x[0-9A-F]+)"[\s]+MESSAGE=
'(.*)'[\s]+\>/>[\s]*(([\s]|.)*?)<\RIBCL>/)
    {
        if($1 eq "0x0000")
        {
            print STDERR "$3\n" if $3;
        }
        else
        {
            print STDERR "ERROR: STATUS: $1, MESSAGE: $2\n";
        }
    }
}
$reply .= $lastreply;
closeSSLconnection($ssl);
return $reply;
}

```

PERL scripts can also send a portion of the XML script, wait for the reply, and send more XML later. Using this technique, it is possible to use the reply produced by an earlier command as input to a later command. However, the PERL script must send data within a few seconds or the device will time out and disconnect.

When using the XML scripting interface with PERL scripts, the following restrictions apply:

- PERL scripts must send the XML header before sending the body of the script.
- PERL scripts must provide script data fast enough to prevent the device from timing out.
- Only one XML document is allowed per connection, which means one pair of RIBCL tags.
- The device will not accept additional XML tags after a syntax error occurs. To send additional XML, a new connection must be established.

Virtual Media scripting

Scripting Web server requirements

Virtual Media scripting uses a media image that is stored and retrieved from a Web server accessible from the management network. The web server must be a HTTP 1.1 compliant server that supports the Range header. Furthermore, for write access to the file, the Web server should support DAV and must support the Content-Range header for DAV transactions. If the Web server does not meet the requirements for DAV, a helper CGI program may be used. The Web server may optionally be configured for basic HTTP authentication SSL support, or both.

Web Server	Read Support	Write Support	Authorization	SSL Support
Microsoft® IIS 5.0	Yes	Yes*	Not tested	Not Tested
Apache	Yes	Yes	Yes	Yes
Apache/Win32	Yes	Yes	Yes	Yes

*IIS does not support Content-Range for DAV transactions. A CGI helper program must be used for write support.

Using virtual media scripting

Virtual media scripting is a method for controlling virtual media devices without going through the browser. Scriptable virtual media supports insert, eject, and status commands for floppy, USB key, and CD/DVD-ROM images.

Virtual media scripting enables you to use methods other than a browser to configure iLO 2 for virtual media use. iLO 2 can be configured remotely using CPQLOCFG XML commands, locally using HPONCFG XML commands, or locally using the HPLOVM utility that replaces the VFLOP utility from the SmartStart Scripting toolkit.

NOTE: Virtual media scripting does not operate Virtual Media using the browser. Likewise, the browser does not support scripting capabilities. For example, a floppy disk mounted using the browser cannot later be dismounted using the scripting interface.

The XML commands enable you to configure virtual media in the same manner as the virtual media applet. However, the actual image is located on a Web server on the same network as iLO 2. After the image location is configured, iLO 2 retrieves the virtual media data directly from the web server.

NOTE: USB key drives must be used with the floppy keyword syntax.

HPLOVM.EXE is a new scripting utility that enables you to script insert, eject, and set boot options for virtual media devices. HPLOVM is intended to be used in place of the VFLOP.exe utility, which is part of the SmartStart Scripting Toolkit.

Command line syntax:

```
HPLOVM [-device <floppy | cdrom>] [-insert <url>] [-eject] [-wp <y | n>]  
[-boot <once | always | never>] [-mgmt <ilo | rilo>] [-ver] [-?]
```

Command Line Input	Result
[-device <floppy cdrom>]	Defines which virtual media device is active.
[-insert <url>]	Defines the location of the virtual media image to connect.
[-eject]	Ejects the media that is currently connected through the virtual media drive. The virtual media drive is still connected, but no media is present in the drive.
[-wp <y n>]	Defines the write-protected status of the Virtual Floppy/USB key drive. This argument has no effect on the Virtual CD-ROM drive.
[-boot <once always never>]	Defines how the virtual media drive is used to boot the target server.
[-mgmt <ilo rilo>]	Defines which management processor is being used with LOVM utility. If RILOE is specified, the VFLOP.EXE utility is used. The default setting of this argument is iLO 2.
[-ver]	Displays the HPLOVM utility version.
[-?]	Displays help information.

Using Virtual Media on Linux servers through an SSH connection

1. Log in to the iLO 2 through SSH (SSH connection from another Linux system, using PuTTY from Windows®).
2. Enter `vm` to display a list of commands available for Virtual Media.
3. Enter `vm floppy insert http://<address>/<image-name>`.
The image is available to boot from, but will not be seen by the operating system. (Boot options can be configured with `vm floppy set <option>`, the options are `boot_once`, `boot_always`, and `no_boot`.) Boot options from a USB key drive are only valid on servers with ProLiant USB key drive support.
4. Enter `vm floppy set connect` to make the floppy or key drive available to the operating system.
5. Enter `vm floppy get` to display the current status. For example:
VM Applet = Disconnected
Boot Option = BOOT_ONCE
Write Protect = Yes
Image Inserted = Connected
The status of the Virtual Media applet is always disconnected, unless a Virtual Floppy/USBKey or CD-ROM is connected through the graphical iLO 2 interface.

The Virtual Floppy/USBKey can be disconnected using the `vm floppy set disconnect` or `vm floppy eject` commands. To connect or disconnect a Virtual CD-ROM, use `cdrom` instead of `floppy`.

The link to the Virtual Floppy/USBKey or CD-ROM image must be a URL. It is not possible to specify a drive letter. The CD-ROM image should be in .iso format. The floppy image can be created from a physical floppy by using `rawrite` or the image creation tool included with the Virtual Media applet in the graphical iLO 2 interface.

Mounting Virtual Media on the Linux server:

1. Use `lsmod` to check that the following modules are loaded:

- o `usbcore`
- o `usb-storage`
- o `usb-ohci`
- o `sd_mod`

If any of the modules are missing, use `modprobe <module>` to load them.

2. Mount the drive using one of following:

- o `mount /dev/sda /mnt/floppy -t vfat`—Mounts a virtual floppy.
- o `mount /dev/sda1 /mnt/keydrive`—Mounts a virtual USB key drive.
- o `mount /dev/cdrom1 /mnt/cdrom`—Mounts a virtual CD-ROM on a Red Hat system. (Use `/dev/cdrom` if the server does not have a locally attached CD-ROM drive.)
- o `mount /dev/scd0 /mnt/cdrom`—Mounts a virtual CD-ROM on a SUSE system.

Virtual media image files

Valid diskette images may be raw disk images, produced by the iLO 2 Virtual Media applet, the UNIX® utility `dd`, the DOS utility `rawrite`, or images created by the CPQIMAGE utility. CD-ROM images must be ISO-9660 file system images. No other type of CD-ROM images are supported.

The images created by the Virtual Media applet are raw disk images in the case of diskettes and ISO-9660 images in the case of CD-ROMs. Many CD-ROM burning utilities can create ISO-9660 images. Refer to the documentation of your utility for additional information.

CGI helper application

The following perl script is an example of a CGI helper application that allows diskette writes on Web servers that cannot perform partial writes. When using the helper application, the iLO 2 firmware posts a request to this application with three parameters:

- The file parameter contains the name of the file provided in the original URL.
- The range parameter contains an inclusive range (in hexadecimal) designating where to write the data.
- The data parameter contains a hexadecimal string representing the data to be written.

The helper script must transform the file parameter into a path relative to its working directory. This function might involve prefixing it with `"../,"` or it might involve transforming an aliased URL path into the true path on the file system. The helper script requires write access to the target file. Diskette image files must have the appropriate permissions.

Example:

```
#!/usr/bin/perl

use CGI;
use Fcntl;

#
# The prefix is used to get from the current working
# directory to the location of the image file#
my ($prefix) = "..";
my ($start, $end, $len, $decode);

# Get CGI data
my $q = new CGI();
# Get file to be written
my $file = $q->param('file');

# Byte range
$range = $q->param('range');

# And the data
my $data = $q->param('data');
#
# Change the filename appropriately
#
$file = $prefix . "/" . $file;

#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
    $start = hex($1);
    $end = hex($2);
    $len = $end - $start + 1;
}

#
# Decode the data (it's a big hex string)
#
$decode = pack("H*", $data);

#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);
```

Setting up IIS for scripted virtual media

Before setting up IIS for scripted media, make sure IIS is operational. Use Internet Information Services (IIS) Manager to set up a simple website and verify that it is working correctly by browsing to the site.

1. Configure IIS to serve diskette or ISO-9660 CD-ROM images for read-only access.
 - a. Add a directory to your website and place your images in the directory.


```

#
# The prefix is used to get from the current working directory
# to the location of the image file you are writing
#
my ($prefix) = "c:/inetpub/wwwroot";
my ($start, $end, $len, $decode);

my $q = new CGI();          # Get CGI data

my $file = $q->param('file'); # File to be written
my $range = $q->param('range'); # Byte range to be written
my $data = $q->param('data'); # Data to be written

#
# Merges the filename correctly
#
$file = $prefix . "/" . $file;

#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
    $start = hex($1);
    $end = hex($2);
    $len = $end - $start + 1;
}

#
# Decode the data (a large hex string)
#
$decode = pack("H*", $data);

#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);

print "Content-Length: 0\r\n";
print "\r\n";

```

HPONCFG online configuration utility

HPONCFG

The HPONCFG utility is an online configuration tool used to set up and configure the iLO, iLO 2, and RILOE II from within Windows® and Linux operating systems without requiring a reboot of the server operating system. The utility runs in a command line mode and must be executed from an operating system command line using an account with administrator or root access. The HPONCFG utility also provides a limited graphical interface for servers that use Windows operating systems.

HPONCFG supported operating systems

- Windows
 - Windows Server® 2003
 - Windows Server® 2008
- RedHat Linux
 - Red Hat Linux Enterprise Linux 3
 - Red Hat Linux Enterprise Linux 4
 - Red Hat Linux Enterprise Linux 5
- SUSE Linux
 - SUSE Linux Enterprise Server 9
 - SUSE Linux Enterprise Server 10
 - SUSE Linux Enterprise Server 11

HPONCFG requirements

- Windows-based servers—The iLO Management Interface Driver must be loaded on the server. The SmartStart operating system installation process normally installs this driver. During execution, HPONCFG issues a warning if it cannot locate the driver. If the driver is not installed, you must download and install the driver on the server. You can download the driver from the HP website (<http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=1135772&prodTypeId=18964&prodSeriesId=1146658&swLang=8&taskId=135&swEnvOID=1005#113213>).
- Linux-based servers—The iLO Management interface driver (hpilo) must be loaded on the server and the health driver package (hp-health rpm) must be installed. The SmartStart operating system installation process normally installs this driver. If the driver is not installed, you must download and install the driver on the server. You can download the driver from the HP website (<http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?prodNameId=1135772&lang=en&cc=us&taskId=135&prodTypeId=18964&prodSeriesId=1146658>)

Installing HPONCFG

The HPONCFG utility is delivered in separate packages for Windows® and Linux operating systems. For Windows® operating systems, it is included as a smart component. For Linux operating systems, it is included as an RPM package file. HPONCFG packages are included in the ProLiant Support Pack.

Windows server installation

HPONCFG installs automatically when the ProLiant Support Pack is installed. To install HPONCFG manually, run the self-extracting executable. HPONCFG creates a directory at %Program files%\HP\hponcfg.

Linux server installation

HPONCFG is installed automatically when ProLiant Support Pack is installed. The rpm of HPONCFG for Linux distributions can be downloaded from the HP website (<http://h20000.www2.hp.com/bizsupport/TechSupport/DriverDownload.jsp?prodNameId=1135772&lang=en&cc=us&taskId=135&prodClassId=1&prodTypeId=18964&prodSeriesId=1146658>).

Install the appropriate package using the rpm installation utility. For example, for a package installation, you can install hponcfg rpm on Red Hat Enterprise Linux 3 by entering the following command:

```
rpm -ivh hponcfg-1.9.0-3.linux.rpm
```

If an older version of the hponcfg RPM package is installed on the system, run the following command to remove the older version before installing the new version of HPONCFG:

```
rpm -e hponcfg
```

The iLO or RILOE II driver (hp-ilo or hprsm) rpm package and the hp-health rpm package must be installed on the system before installing the hponcfg rpm package.

After installation, the HPONCFG executable is located in the /sbin directory. Be sure that the appropriate Management Interface Driver is installed. See the section, "HPONCFG requirements (on page 61)" for details about where to obtain this driver and file.

HPONCFG utility

The HPONCFG configuration utility reads an XML input file, formatted according to the rules of the RIBCL language, and produces a log file containing the requested output. A few sample scripts are included in the HPONCFG delivery package. A package containing various and comprehensive sample scripts is available for download on the HP website

(<http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareIndex.jsp?lang=en&cc=us&prodNameId=1135772&prodTypeId=18964&prodSeriesId=1146658&swLang=8&taskId=135&swEnvOID=1005#113213>).

Typical usage is to select a script that is similar to the desired functionality and modify it for your exact requirements. Although no authentication to iLO, iLO 2, or RILOE II is required, the XML syntax requires that the USER_LOGIN and PASSWORD tags are present in the LOGIN tag, and that these fields contain data. Any data is accepted in these fields. To successfully execute HPONCFG, the utility must be invoked as Administrator on Windows® servers and as root on Linux servers. HPONCFG returns an error message, if you do not possess sufficient privileges.

HPONCFG command line parameters

HPONCFG accepts the following command line parameters:

- `/help` or `?`—Displays the help page.
- `/reset`—Resets the RILOE II, iLO, or iLO 2 to factory default values.
- `/f <filename>`—Sets and receives the RILOE II, iLO, or iLO 2 configuration from the information given in the XML input file that has name *filename*.
- `/i <filename>`—Sets and receives RILOE II, iLO or iLO2 configuration from XML input received through the standard input stream.
- `/w <filename>`—Writes the RILOE II, iLO, or iLO 2 configuration obtained from the device to the XML output file that has the name *filename*.
- `/l <filename>`—Logs replies to the text log file that has name *filename*.
- `/s <namevaluepairs>` or `/substitute <namevaluepairs>`—Substitutes variables present in the input config file with values specified in *<namevaluepairs>*.
- `/get_hostinfo`—Receives the host information. Returns the server name and server serial number.
- `/m`—Indicates the minimum firmware level that should be present in the management device to execute the RIBCL script. If at least this level of firmware is not present, HPONCFG returns an error without performing any additional action.
- `/mouse`—Configures the server for optimized mouse handling to improve graphical remote console performance. By default, it optimizes for remote console single cursor mode for the current user. The `dualcursor` command line option, along with the mouse option, optimizes mouse handling as suited for remote console dual-cursor mode. The `allusers` command line option optimizes mouse handling for all users on the system. This option is available only for Windows®.
- `/display`—Configures Windows® display parameters to optimize graphical remote console display performance.

The options must be preceded by a / (slash) for Windows® and Linux as specified in the usage string.

Example HPONCFG command line:

```
HPONCFG /f add_user.xml /l log.txt > output.txt
```

Using HPONCFG on Windows servers

Start the HPONCFG configuration utility from the command line. When using Windows®, `cmd.exe` is available by selecting **Start>Run>cmd**. HPONCFG displays a usage page if HPONCFG is entered with no command line parameters. HPONCFG accepts a correctly formatted XML script. For more information about formatting XML scripts, see "Using RIBCL (on page 70)." HPONCFG sample scripts are included in the HPONCFG package.

The command line format is:

```
HPONCFG [ /help | /? | /m firmwarelevel | /reset [/m firmwarelevel]
        | /f filename [/l filename] [/s namevaluepairs]
        [/xmlverbose or /v] [/m firmwarelevel]
        | /i [/l filename] [/s namevaluepairs]
        [/xmlverbose or /v] [/m firmwarelevel]
        | /w filename [/m firmwarelevel]
        | /get_hostinfo [/m firmwarelevel]
```

```
| /mouse [/dualcursor][/allusers] ]
```

For more information on using these parameters, see "HPONCFG command line parameters (on page 63)."

Using HPONCFG on Linux servers

Invoke the HPONCFG configuration utility from the command line. HPONCFG displays a usage page if it is entered with no command line parameters.

The command line format is:

```
hponcfg -?
hponcfg -h
hponcfg -m minFw
hponcfg -r [-m minFw ]
hponcfg -w filename [-m minFw]
hponcfg -g [-m minFw]
hponcfg -f filename [-l filename] [-s namevaluepairs] [-v] [-m minFw]
hponcfg -i [-l filename] [-s namevaluepairs] [-v] [-m minFw]
```

For more information on using these parameters, see "HPONCFG command line parameters (on page 63)."

Obtaining the basic configuration

You can use HPONCFG to obtain a basic configuration from RILOE II, iLO, or iLO 2 by executing the utility from the command line without specifying an input file. You must provide the name of the output file on the command line. For example:

```
HPONCFG /w config.xml
```

In this example, the utility indicates that it obtained the data successfully and wrote the data to the output file. The following is a typical example of the contents of the output file:

```
<!-- HPONCFG VERSION = "1.2" -->
<!-- Generated 07/06/05 09:06:51 -->
<RIBCL VERSION="2.1">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<DIR_INFO MODE="write">
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
<DIR_LOCAL_USER_ACCT VALUE = "Y"/>
<DIR_SERVER_ADDRESS VALUE = ""/>
<DIR_SERVER_PORT VALUE = "636"/>
<DIR_OBJECT_DN VALUE = ""/>
<DIR_OBJECT_PASSWORD VALUE = ""/>
<DIR_USER_CONTEXT_1 VALUE = ""/>
<DIR_USER_CONTEXT_2 VALUE = ""/>
<DIR_USER_CONTEXT_3 VALUE = ""/>
</MOD_DIR_CONFIG>
</DIR_INFO>
<RIB_INFO MODE="write">
<MOD_NETWORK_SETTINGS>
<SPEED_AUTOSELECT VALUE = "Y"/>
<NIC_SPEED VALUE = "100"/>
<FULL_DUPLEX VALUE = "Y"/>
<DHCP_ENABLE VALUE = "Y"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
```



```

<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "N"/>
<IP_ADDRESS VALUE = "16.100.241.229"/>
<SUBNET_MASK VALUE = "255.255.252.0"/>
<GATEWAY_IP_ADDRESS VALUE = "16.100.240.1"/>
<DNS_NAME VALUE = "ILOD234KJ44D002"/>
<DOMAIN_NAME VALUE = "americas.cpqcorp.net"/>
<PRIM_DNS_SERVER value = "16.81.3.242"/>
<SEC_DNS_SERVER value = "0.0.0.0"/>
<TER_DNS_SERVER value = "0.0.0.0"/>
<PRIM_WINS_SERVER value = "16.81.3.247"/>
<SEC_WINS_SERVER value = "0.0.0.0"/>
<STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
</MOD_NETWORK_SETTINGS>
<USER_INFO MODE="write">
<ADD_USER
    USER_NAME = "Username1"
    USER_LOGIN = "User1"
    PASSWORD = "%user_password%">
<ADMIN_PRIV value = "N"/>
<REMOTE_CONS_PRIV value = "Y"/>
<RESET_SERVER_PRIV value = "N"/>
<VIRTUAL_MEDIA_PRIV value = "N"/>
<CONFIG_ILO_PRIV value = "N"/>
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

```

For security reasons, user passwords are not returned.

Obtaining a specific configuration

A specific configuration can be obtained using the appropriate XML input file. For example, the following is the contents of a typical XML input file, `get_global.xml`:

```

<!-- Sample file for Get Global command -->
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
    <RIB_INFO MODE="read">
        <GET_GLOBAL_SETTINGS />
    </RIB_INFO>
</LOGIN>
</RIBCL>

```

The XML commands are read from the input file `get_global.xml` and are processed by the device:

```
HPONCFG /f get_global.xml /l log.txt > output.txt
```

The requested information is returned in the log file, which, in this example, is named `log.txt`.

```

<GET_GLOBAL_SETTINGS>
    <SESSION_TIMEOUT VALUE="15"/>
    <ILO_FUNCT_ENABLED VALUE="Y"/>
    <F8_PROMPT_ENABLED VALUE="Y"/>

```

```

<F8_LOGIN_REQUIRED VALUE="N"/>
<TELNET_ENABLE VALUE="N"/>
<PASSTHROUGH_CONFIG VALUE="1"/>
<HTTPS_PORT VALUE="443"/>
<HTTP_PORT VALUE="80"/>
<REMOTE_CONSOLE_PORT VALUE="23"/>
<TERMINAL_SERVICES_PORT VALUE="3389"/>
<VIRTUAL_MEDIA_PORT VALUE="17988"/>
<SSH_PORT VALUE="22"/>
<SSH_STATUS VALUE="Y"/>
<SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
<SERIAL_CLI_SPEED VALUE="9600"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<REMOTE_KEYBOARD_MODEL VALUE="US"/>
<RBSU_POST_IP VALUE="Y"/>
<HIGH_PERFORMANCE_MOUSE VALUE="Automatic">
<REMOTE_CONSOLE_ACQUIRE VALUE="N"/>
</GET_GLOBAL_SETTINGS>

```

Setting a configuration

You can set a specific configuration by using the command format:

```
HPONCFG /f add_user.xml /l log.txt
```

In this example, the input file has contents:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<USER_INFO MODE="write">
  <ADD_USER
    USER_NAME="Landy9"
    USER_LOGIN="mandy8"
    PASSWORD="floppyshoes">
    <ADMIN_PRIV value ="No"/>
    <REMOTE_CONS_PRIV value ="Yes"/>
    <RESET_SERVER_PRIV value ="No"/>
    <VIRTUAL_MEDIA_PRIV value ="No"/>
    <CONFIG_ILO_PRIV value="Yes"/>
  </ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

```

The specified user is added to the device.

Using variable substitution

HPONCFG version 1.2 and greater enables you to specify variables in the XML RIBCL script and to assign values to those variables when HPONCFG is executed. This feature helps to avoid rewriting the XML script file every time with different values. Anything enclosed by two '%' characters in the XML file is considered a variable.

Example 1: In this example, %username%, %loginname%, and %password% are variables.

```
<!-- Add user with minimal privileges to test default setting of
assigned privileges to 'N' -->
<RIBCL version="1.2">
  <LOGIN USER_LOGIN="x" PASSWORD="x">
    <USER_INFO MODE="write">
      <ADD_USER USER_NAME="%username%" USER_LOGIN="%loginname%"
        PASSWORD="%password%">
      <RESET_SERVER_PRIV value="Y" />
      <ADMIN_PRIV value="Y" />
    </ADD_USER>
  </USER_INFO>
</LOGIN>
</RIBCL>
```

You can specify values for these variables at execution time using the substitute option. The argument must be a string or variable name and value pairs separated by delimiter ',' (comma). The variable name and its value must be separated by an equal sign (=).

```
HPONCFG /f add_user.xml /s username="test
user",login="testlogin",password=testpasswd
```

Example 2: In this example, %host_power% is a variable.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <!-- Modify the HOST_POWER attribute to toggle power on the host server
      -->
      <!-- HOST_POWER="No" (Turns host server power off) -->
      <!-- A graceful shutdown will be attempted for ACPI-aware -->
      <!-- operating systems configured to support graceful shutdown. -->
      <!-- HOST_POWER="Yes" (Turns host server power on) -->
      <SET_HOST_POWER HOST_POWER="%host_power%"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

- To power on the system, enter `HPONCFG /f Set_Host_Power.xml /s host_power=YES.`
- To power off the system, enter `HPONCFG /f Set_Host_Power.xml /s host_power=NO.`

Capturing and restoring a configuration

You can use HPONCFG to capture basic configuration information in an XML readable file format and use the file to set or restore the configuration of the management processor. This feature is available with HPONCFG version 1.2 and greater which writes the configuration information in HP RIBCL format.

- To capture a configuration, you must specify the name and location of the output file on the command line. For example:
`HPONCFG /w config.xml`

The utility displays a message when it successfully writes the configuration information to the output file as requested. The following is an example of the contents of the output file:

```
<!-- HPONCFG VERSION = "1.2" -->
<!-- Generated 07/06/05 09:06:51 -->
<RIBCL VERSION="2.1">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<DIR_INFO MODE="write">
  <MOD_DIR_CONFIG>
    <DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
    <DIR_LOCAL_USER_ACCT VALUE = "Y"/>
    <DIR_SERVER_ADDRESS VALUE = ""/>
    <DIR_SERVER_PORT VALUE = "636"/>
    <DIR_OBJECT_DN VALUE = ""/>
    <DIR_OBJECT_PASSWORD VALUE = ""/>
    <DIR_USER_CONTEXT_1 VALUE = ""/>
    <DIR_USER_CONTEXT_2 VALUE = ""/>
    <DIR_USER_CONTEXT_3 VALUE = ""/>
  </MOD_DIR_CONFIG>
</DIR_INFO>
<RIB_INFO MODE="write">
  <MOD_NETWORK_SETTINGS>
    <SPEED_AUTOSELECT VALUE = "Y"/>
    <NIC_SPEED VALUE = "100"/>
    <FULL_DUPLEX VALUE = "Y"/>
    <DHCP_ENABLE VALUE = "Y"/>
    <DHCP_GATEWAY VALUE = "Y"/>
    <DHCP_DNS_SERVER VALUE = "Y"/>
    <DHCP_STATIC_ROUTE VALUE = "Y"/>
    <DHCP_WINS_SERVER VALUE = "Y"/>
    <REG_WINS_SERVER VALUE = "N"/>
    <IP_ADDRESS VALUE = "16.100.241.229"/>
    <SUBNET_MASK VALUE = "255.255.252.0"/>
    <GATEWAY_IP_ADDRESS VALUE = "16.100.240.1"/>
    <DNS_NAME VALUE = "ILOD234KJ44D002"/>
    <DOMAIN_NAME VALUE = "americas.cpqcorp.net"/>
    <PRIM_DNS_SERVER value = "16.81.3.242"/>
    <SEC_DNS_SERVER value = "0.0.0.0"/>
    <TER_DNS_SERVER value = "0.0.0.0"/>
    <PRIM_WINS_SERVER value = "16.81.3.247"/>
    <SEC_WINS_SERVER value = "0.0.0.0"/>
    <STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
    <STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
    <STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
  </MOD_NETWORK_SETTINGS>
</RIB_INFO>
<USER_INFO MODE="write">
  <ADD_USER
```

```

    USER_NAME = "Username1"
    USER_LOGIN = "User1"
    PASSWORD = "%user_password%">
    <ADMIN_PRIV value = "N"/>
    <REMOTE_CONS_PRIV value = "Y"/>
    <RESET_SERVER_PRIV value = "N"/>
    <VIRTUAL_MEDIA_PRIV value = "N"/>
    <CONFIG_ILO_PRIV value = "N"/>
  </ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>

```

The default user Administrator and user passwords are not captured in the configuration file or returned in the response for security reasons. A variable is provided in its place which you can use with the substitute option to provide a default password for all users when restoring a configuration. You can also manually change the password before using the file to restore the configuration.

- To restore the configuration, the file must be sent to HPONCFG as input to the `/f` or `-f` option. You can add a default password for all the users using the substitute or `s` option. For example:
`HPONCFG /f config.xml /s user_password=password`

Using RIBCL

Overview of the RIBCL

RIBCL enables you to write XML scripts to configure and manage iLO 2 configuration settings, user accounts, directory settings, server settings, and HP SIM SSO settings. You can download sample scripts for all iLO 2 commands described in this section from the HP website (<http://www.hp.com/servers/lights-out>). Before using the XML sample scripts downloaded from the HP website, read the firmware support information in each sample script to tailor the script for the intended firmware and version.

When writing your XML scripts, do write comments in the command. If a comment falls in the command line, an error message is generated. Unless otherwise specified, examples in this guide are specifically for iLO 2 firmware version 1.10 and later.

The "Using RIBCL" section describes the XML commands and their parameters common to most LOM products and servers. For more information about the ProLiant BL p-class server and rack XML commands, see the *HP Integrated Lights-Out 2 User Guide*.

XML header

The XML header ensures the connection is an XML connection, not an HTTP connection. The XML header is built into the cpqlocfg utility and has the following format:

```
<?xml version="1.0"?>
```

Data types

The three data types that are allowed in the parameter are:

- String
- Specific string
- Boolean string

String

A string is any text enclosed in quotes. It can include spaces, numbers, or any printable character. A string may start with either a double or single quote and it must end with the same type of quote. The string may contain a quote if it is different from the string delimiter quotes.

For example, if a string is started with a double quote, a single quote can be used within the string and the string must be closed with a double quote.

Specific string

A specific string is one that is required to contain certain characters. In general, you have a choice of words that are accepted as correct syntax and all other words produce an error.

Boolean string

A Boolean string is a specific string that specifies a "yes" or "no" condition. Acceptable Boolean strings are "yes," "y," "no," "n," "true," "t," "false," and "f." These strings are not case sensitive.

Response definitions

Every command that is sent to the iLO 2 generates a response. The response indicates whether the command succeeded or failed. Some commands generate additional information. The additional information is displayed in execution sequence, provided no errors occurred.

Example:

```
<RESPONSE
  STATUS="0x0001"
  MSG="There has been a severe error."
/>
```

- **RESPONSE**
This tag name indicates that the iLO 2 is sending a response to the previous commands back to the client application to indicate the success or failure of the commands that have been sent to the iLO 2.
- **STATUS**
This parameter contains an error number. The number 0x0000 indicates that there is no error.
- **MSG**
This element contains a message describing the error that happened. If no error occurred, the message `No error` appears.

RIBCL

This command is used to start and end an RIBCL session. You can use it only once to start an RIBCL session, and it must be the first command to display in the script. The RIBCL tags are required to mark the beginning and the end of the RIBCL document.

Example:

```
<RIBCL VERSION="2.0">
</RIBCL>
```

RIBCL parameters

VERSION is a string that indicates the version of the RIBCL that the client application is expecting to use. The VERSION string is compared to the version of the RIBCL that is expected, and an error is returned if the string and the version do not match. The preferred value for the VERSION parameter is "2.0." The VERSION parameter is no longer checked for an exact match; however, this parameter can never be blank.

RIBCL runtime errors

The possible RIBCL error messages include:

Version must not be blank.

LOGIN

The LOGIN command provides the information that is used to authenticate the user whose permission level will be used when performing RIBCL actions. The specified user must have a valid account on the respective iLO 2 to execute RIBCL commands. The user's privileges are checked against the required privilege for a particular command, and an error is returned if the privilege level does not match.

Example:

```
<LOGIN USER_LOGIN="username" PASSWORD="password">
</LOGIN>
```

Alternatively, the CPQLOCFG utility can specify the login information as parameters on its command line:

```
cpqlocfg -u <username> -p <password>
```

When using this format, the utility returns an `Overriding credentials` warning message but still shows the error log message entry as `Login name must not be blank.`

LOGIN parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters.

LOGIN runtime errors

The possible runtime error messages include:

- User login name was not found.
- Password must not be blank.
- Logged-in user does not have required privilege for this command.

USER_INFO

The USER_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local user information database into memory and prepares to edit it. Only commands that are USER_INFO type commands are valid inside the USER_INFO command block. The USER_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If database is open for writing by another application, then this call will fail.

USER_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO 2 information. Read mode prevents modification of the iLO 2 information.

Example:

```
<USER_INFO MODE="write">
..... USER_INFO commands .....
</USER_INFO>
```


ADD_USER

The ADD_USER command is used to add a local user account. The USER_NAME and USER_LOGIN parameters must not exist in the current user database. Use the MOD_USER command to change an existing user's information. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

All of the attributes that pertain to the user are set using the following parameters.

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="loginname" PASSWORD="password">
    <USER_INFO MODE="write">
      <ADD_USER
        USER_NAME="User"
        USER_LOGIN="username" PASSWORD="password">
        <ADMIN_PRIV value ="No"/>
        <REMOTE_CONS_PRIV value ="Yes"/>
        <RESET_SERVER_PRIV value ="No"/>
        <VIRTUAL_MEDIA_PRIV value ="No"/>
        <CONFIG_ILO_PRIV value ="No"/>
      </ADD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

ADD_USER parameters

USER_NAME is the actual name of the user. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

USER_LOGIN is the name used to gain access to the respective iLO 2. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO 2 Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user

should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_ILO_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current iLO 2 configuration.

The following parameters are not applicable to a user's privileges in the iLO firmware versions 1.40 and higher and iLO 2 firmware versions 1.1x and higher. The parameters will parse correctly, but user privileges will not be affected.

VIEW_LOGS_PRIV is a Boolean parameter that gives the user permission to view the iLO 2 system logs. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to view logs. If this parameter is used, the Boolean string value must never be blank.

CLEAR_LOGS_PRIV is a Boolean parameter that gives the user permission to clear the event log. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to clear the iLO 2 event log. If this parameter is used, the Boolean string value must never be blank.

EMS_PRIV is a Boolean parameter that gives the user permission to use the Windows® Server 2003 EMS service. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to use EMS services. If this parameter is used, the Boolean string value must never be blank.

UPDATE_ILO_PRIV is a Boolean parameter that allows the user to copy a new firmware image into the iLO 2 system ROM. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to configure iLO 2. If this parameter is used, the Boolean string value must never be blank.

CONFIG_RACK_PRIV is a Boolean parameter that gives the user permission to configure and manage the server rack resources. This parameter is applicable to ProLiant BL p-Class servers only. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to manage or configure rack resources. If this parameter is used, the Boolean string value must never be blank.

DIAG_PRIV is a Boolean parameter that gives the user permission to view diagnostic information about iLO 2. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have diagnostic privileges. If this parameter is used, the Boolean string value must never be blank.

ADD_USER runtime errors

The possible ADD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.
- User table is full. No room for new user.
- Cannot add user. The user name already exists.
- User information is open for read-only access. Write access is required for this operation.

- User name cannot be blank.
- User login ID cannot be blank.
- Boolean value not specified.
- User does not have correct privilege for action. ADMIN_PRIV required.

DELETE_USER

The DELETE_USER command is used to remove an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname"
    PASSWORD="password">
    <USER_INFO MODE="write">
      <DELETE_USER USER_LOGIN="username"/>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

DELETE_USER parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

DELETE_USER runtime errors

The possible DELETE_USER errors include:

- User information is open for read-only access. Write access is required for this operation.
- Cannot delete user information for currently logged in user.
- User login name was not found.
- User login name must not be blank.
- User does not have correct privilege for action. ADMIN_PRIV required.

DELETE_CURRENT_USER

The DELETE_CURRENT_USER command is used to remove the user account defined by the USER_LOGIN attribute. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

This command is intended for customers who desire to delete all user accounts on iLO 2.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname"
```

```

        PASSWORD="password">
        <USER_INFO MODE="write">
        <DELETE_CURRENT_USER/>
        </USER_INFO>
    </LOGIN>
</RIBCL>

```

DELETE_CURRENT_USER parameters

None

DELETE_CURRENT_USER runtime errors

The possible DELETE_CURRENT_USER errors include:

User information is open for read-only access. Write access is required for this operation.

GET_USER

The GET_USER command will return a local user's information, excluding the password. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve other user accounts; else the user can only view their individual account information.

Example:

```

<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
    <GET_USER USER_LOGIN="username"/>
    </USER_INFO>
    </LOGIN>
</RIBCL>

```

GET_USER parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

GET_USER runtime errors

The possible GET_USER error messages include:

- User login name must not be blank.
- User login name was not found.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_USER return messages

A possible GET_USER return message includes:

```
<RESPONSE
```

```

    STATUS="0x0000"
    MSG="No Errors"
  />

  <GET_USER
    USER_NAME="Admin User"
    USER_LOGIN= "username"
    ADMIN_PRIV="N"
    REMOTE_CONS_PRIV="Y"
    RESET_SERVER_PRIV="N"
    VIRTUAL_MEDIA_PRIV="N"
    CONFIG_ILO_PRIV value ="No"
  />

```

MOD_USER

The MOD_USER command is used to modify an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege. A user without the administrative privilege can only modify their individual account password.

Example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="write">
      <MOD_USER USER_LOGIN="loginname">
        <USER_NAME value="username"/>
        <USER_LOGIN value="newloginname"/>
        <PASSWORD value="password"/>
        <ADMIN_PRIV value="No"/>
        <REMOTE_CONS_PRIV value="Yes"/>
        <RESET_SERVER_PRIV value="No"/>
        <VIRTUAL_MEDIA_PRIV value="No"/>
        <CONFIG_ILO_PRIV value="Yes"/>
      </MOD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>

```

Reset administrator password example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="write">
      <MOD_USER USER_LOGIN="Administrator">
        <PASSWORD value="password"/>
      </MOD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>

```

Change password example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="write">
      <MOD_USER USER_LOGIN="username">
        <PASSWORD value="newpassword"/>
      </MOD_USER>
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

MOD_USER parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

If the following parameters are not specified, then the parameter value for the specified user is preserved.

USER_NAME is the actual name of the user to be added. This parameter is case sensitive, can be any valid string, and has a maximum length of 39 characters. This string is used for display only and must never be blank.

USER_LOGIN is the name used to gain access to the respective iLO 2. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 39 characters. The minimum length is defined in the iLO 2 Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_ILO_PRIV is a Boolean parameter that allows the user to configure iLO settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current iLO 2 configuration.

MOD_USER runtime errors

The possible MOD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.
- User information is open for read-only access. Write access is required for this operation.
- User login name must not be blank.
- Cannot modify user information for currently logged user.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS

The GET_ALL_USERS command will return all USER_LOGIN parameters in the user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve all user accounts.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
      <GET_ALL_USERS />
    </USER_INFO>
  </LOGIN>
</RIBCL>
```

GET_ALL_USERS parameters

None

GET_ALL_USERS runtime errors

The possible GET_ALL_USERS error messages include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS return messages

A possible GET_ALL_USERS return message is:

```
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No Error'
/>
<GET_ALL_USERS>
  <USER_LOGIN VALUE="username"/>
  <USER_LOGIN VALUE="user2"/>
  <USER_LOGIN VALUE="user3"/>
```

```

<USER_LOGIN VALUE="user4"/>
<USER_LOGIN VALUE="user5"/>
<USER_LOGIN VALUE="user6"/>
<USER_LOGIN VALUE="user7"/>
<USER_LOGIN VALUE="user8"/>
<USER_LOGIN VALUE="user9"/>
<USER_LOGIN VALUE="user10"/>
<USER_LOGIN VALUE="" />
<USER_LOGIN VALUE="" />
</GET_ALL_USERS>

```

A possible unsuccessful request is:

```

<RESPONSE
  STATUS="0x0023"
  MESSAGE='User does NOT have correct privilege for action. ADMIN_PRIV
  required.'
/>

```

GET_ALL_USER_INFO

The GET_ALL_USER_INFO command will return all local users information in the user database, excluding passwords. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have administrative privilege to execute this command.

Example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
      <GET_ALL_USER_INFO />
    </USER_INFO>
  </LOGIN>
</RIBCL>

```

GET_ALL_USER_INFO parameters

None

GET_ALL_USER_INFO runtime errors

The possible GET_ALL_USER_INFO error message include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USER_INFO return messages

A possible GET_ALL_USER_INFO return message is:

```

<GET_ALL_USER_INFO/>
<GET_USER

```



```

    USER_NAME="Admin"
    USER_LOGIN="Admin"
    ADMIN_PRIV="Y"
    CONFIG_RILO_PRIV="Y"
    LOGIN_PRIV="Y"
    REMOTE_CONS_PRIV="Y"
    RESET_SERVER_PRIV="Y"
    VIRTUAL_MEDIA_PRIV="Y"
/> .....
The same information will be repeated for all the users.
</GET_ALL_USER_INFO>

```

A possible unsuccessful request is:

```

<RESPONSE
    STATUS="0x0023"
    MESSAGE='User does NOT have correct privilege for action. ADMIN_PRIV
    required.'
/>

```

RIB_INFO

The RIB_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the iLO 2 configuration information database into memory and prepares to edit it. Only commands that are RIB_INFO type commands are valid inside the RIB_INFO command block. The RIB_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

RIB_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO 2 information. Read mode prevents modification of the iLO 2 information.

Example:

```

<RIB_INFO MODE="write">
..... RIB_INFO commands .....
</RIB_INFO>

```

Clear iLO 2 event log example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
        <CLEAR_EVENTLOG/>
    </RIB_INFO>
</LOGIN>
</RIBCL>

```

RESET_RIB

The RESET_RIB command is used to reset iLO 2. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Admin" PASSWORD="Password">
    <RIB_INFO MODE = "write">
      <RESET_RIB/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

RESET_RIB parameters

None

RESET_RIB runtime errors

The possible RESET_RIB error message include:

User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_EVENT_LOG

The GET_EVENT_LOG command retrieves the iLO 2 Event Log or the Integrated Management log, depending on the context of the command. For this command to parse correctly, the command must appear within a RIB_INFO or SERVER_INFO command block. To retrieve the iLO 2 Event Log, use the RIB_INFO command block. To retrieve the Integrated Management log use, the SERVER_INFO command block.

Examples:

- iLO 2 Event Log example:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="READ">
    <GET_EVENT_LOG />
  </RIB_INFO>
</LOGIN>
</RIBCL>
```
- Integrated Management log example:

```
<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="READ">
    <GET_EVENT_LOG />
  </SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_EVENT_LOG parameters

None

GET_EVENT_LOG runtime errors

GET_EVENT_LOG returns a runtime error if it is not called from within the RIB_INFO or SERVER_INFO block. For example:

```
<RIBCL VERSION="2.21">
  <RESPONSE
    STATUS="0x0001"
    MESSAGE='Syntax error: Line #3: syntax error near ">" in the line: "
      GET_EVENT_LOG >"'
  />
</RIBCL>
```

GET_EVENT_LOG return messages

The response includes all of the events recorded, in the order that they occurred. Events are not sorted by severity or other criteria. Each event includes a common set of attributes:

- SEVERITY indicates the importance of the error and how it might impact server or iLO 2 availability.
 - FAILED indicates a problem or component failure that might impact operational time if it is not addressed.
 - CAUTION indicates an event that is not expected during normal system operation. This might not indicate a platform issue.
 - REPAIRED indicates that an event or component failure has been addressed.
 - INFORMATIONAL indicates that something noteworthy occurred, but operational time is not impacted.
- CLASS indicates the subsystem that generated the event, and can include iLO 2, environment, power, system error, rack infrastructure, and more.
- LAST_UPDATE indicates the most recent time this event was modified.
- INITIAL_UPDATE indicates when this event first occurred.
- COUNT indicates the number of times a duplicate event happened.
- DESCRIPTION indicates the nature of the event and all recorded details.

The following response is typical of the data returned from the iLO 2 Event Log:

```
<EVENT_LOG DESCRIPTION="iLO Event Log">
  <EVENT
    SEVERITY="Caution"
    CLASS="iLO"
    LAST_UPDATE="04/04/2004 12:34"
    INITIAL_UPDATE="04/04/2004 12:34"
    COUNT="1"
    DESCRIPTION="Server reset."
  />
  ...
```

```
</EVENT_LOG>
```

The following response is typical of the data returned from the Integrated Management Log:

```
<EVENT_LOG DESCRIPTION="Integrated Management Log">
  <EVENT
    SEVERITY="Caution"
    CLASS="POST Message"
    LAST_UPDATE="04/04/2004 12:34"
    INITIAL_UPDATE="04/04/2004 12:34"
    COUNT="1"
    DESCRIPTION="POST Error: 1775-Drive Array - ProLiant Storage System
    not Responding"
  />
  ...
</EVENT_LOG>
```

CLEAR_EVENTLOG

The CLEAR_EVENTLOG command clears the iLO 2 Event Log. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <CLEAR_EVENTLOG/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

CLEAR_EVENTLOG parameters

None

CLEAR_EVENTLOG runtime errors

The possible CLEAR_EVENTLOG error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

COMPUTER_LOCK_CONFIG

The COMPUTER_LOCK_CONFIG command is used to configure the Remote Console Computer Lock feature. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. You must have the Configure iLO 2 privilege to execute this command.

Uppercase letters are not supported, and are converted automatically to lowercase. If either a double quote or a single quote is used, it must be different from the delimiter. For a complete list of the supported custom keys, see the *HP Integrated Lights-Out 2 User Guide*.

Windows® example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO_MODE="write">
  <COMPUTER_LOCK_CONFIG>
    <COMPUTER_LOCK value="windows"/>
  </COMPUTER_LOCK_CONFIG>
</RIB_INFO_MODE="write">
</LOGIN>
</RIBCL>
```

Custom example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO_MODE="write">
  <COMPUTER_LOCK_CONFIG>
    <COMPUTER_LOCK value="custom"/>
    <COMPUTER_LOCK key="l_gui,l"/>
  </COMPUTER_LOCK_CONFIG>
</RIB_INFO_MODE="write">
</LOGIN>
</RIBCL>
```

Disabled example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO_MODE="write">
  <COMPUTER_LOCK_CONFIG>
    <COMPUTER_LOCK value="disabled"/>
  </COMPUTER_LOCK_CONFIG>
</RIB_INFO_MODE="write">
</LOGIN>
</RIBCL>
```

COMPUTER_LOCK_CONFIG parameters

The computer lock on Windows®-based operating systems defaults to the Windows® logo + L keys. You can customize Linux and other operating systems by setting the `<COMPUTER_LOCK value="custom"/>` parameter. For example:

```
<COMPUTER_LOCK key="l_gui,l"/>
```

COMPUTER_LOCK_CONFIG runtime errors

The possible COMPUTER_LOCK_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Invalid number of parameters. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.
- Invalid COMPUTER_LOCK option; value must be windows, custom, or disabled.

- COMPUTER_LOCK value must be set to custom to use the COMPUTER_LOCK_KEY tag.
- The COMPUTER_LOCK key command was used without a preceding COMPUTER_LOCK value command equal to custom.
- The key parameter specified is not valid

GET_NETWORK_SETTINGS

The GET_NETWORK_SETTINGS command requests the respective iLO 2 network settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_NETWORK_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_NETWORK_SETTINGS parameters

None

GET_NETWORK_SETTINGS runtime errors

None

GET_NETWORK_SETTINGS return messages

A possible GET_NETWORK_SETTINGS return message is:

```
<ENABLE_NIC VALUE="Y"/>
  <SHARED_NETWORK_PORT VALUE="N"/>
  <VLAN_ENABLED="N"/>
  <VLAN_ID VALUE="0"/>
  <SPEED_AUTOSELECT VALUE="Y"/>
  <NIC_SPEED VALUE="10"/>
  <FULL_DUPLEX VALUE="N"/>
  <DHCP_ENABLE VALUE="Y"/>
  <DHCP_GATEWAY VALUE="Y"/>
  <DHCP_DNS_SERVER VALUE="Y"/>
  <DHCP_WINS_SERVER VALUE="Y"/>
  <DHCP_STATIC_ROUTE VALUE="Y"/>
  <DHCP_DOMAIN_NAME VALUE="Y"/>
  <REG_WINS_SERVER VALUE="Y"/>
  <REG_DDNS_SERVER VALUE="Y"/>
  <PING_GATEWAY VALUE="N"/>
```

```

<MAC_ADDRESS VALUE="00:12:79:a5:25:42"/>
<IP_ADDRESS VALUE="170.100.8.10"/>
<SUBNET_MASK VALUE="255.255.255.0"/>
<GATEWAY_IP_ADDRESS VALUE="170.100.8.254"/>
<DNS_NAME VALUE="ILO000FWDC451"/>
<DOMAIN_NAME VALUE="ferrari.com"/>
<PRIM_DNS_SERVER VALUE="172.25.163.199"/>
<SEC_DNS_SERVER VALUE="0.0.0.0"/>
<TER_DNS_SERVER VALUE="0.0.0.0"/>
<PRIM_WINS_SERVER VALUE="172.25.163.199"/>
<SEC_WINS_SERVER VALUE="0.0.0.0"/>
<STATIC_ROUTE_1 DEST="0.0.0.0"
    GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_2 DEST="0.0.0.0"
    GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_3 DEST="0.0.0.0"
    GATEWAY="0.0.0.0"/>
</GET_NETWORK_SETTINGS>

```

A possible unsuccessful request is:

```

<RESPONSE
    STATUS = "0x0001"
    MSG = "Error Message"/>

```

MOD_NETWORK_SETTINGS

MOD_NETWORK_SETTINGS is used to modify network settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

The iLO 2 scripting firmware does not attempt to decipher if the network modifications are appropriate for the network environment. When modifying network settings, be aware of the network commands provided to the management processor. In some cases, the management processor ignores commands and no error is returned. For example, when a script includes the command to enable DHCP and a command to modify the IP address, the IP address is ignored. Changing the network settings to values that are not correct for the network environment might cause a loss of connectivity to iLO 2.

The iLO 2 management processor reboots to apply the changes after the script has successfully completed. If connectivity to iLO 2 is lost, use RBSU to reconfigure the network settings to values that are compatible with the network environment.

Example:

```

<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
    <MOD_NETWORK_SETTINGS>
        <ENABLE_NIC value="Yes"/>
        <REG_DDNS_SERVER value="Yes"/>
        <PING_GATEWAY value="No"/>
        <DHCP_DOMAIN_NAME value="Yes"/>
    </MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>

```

```

<SPEED_AUTOSELECT value="YES"/>
<NIC_SPEED value="100"/>
<FULL_DUPLEX value="Yes"/>
<DHCP_ENABLE value="No"/>
<IP_ADDRESS value="172.20.60.152"/>
<SUBNET_MASK value="255.255.255.0"/>
<GATEWAY_IP_ADDRESS value="172.20.60.1"/>
<DNS_NAME value="demoilo"/>
<DOMAIN_NAME value="internal.com"/>
<DHCP_GATEWAY value="Yes"/>
<DHCP_DNS_SERVER value="Yes"/>
<DHCP_WINS_SERVER value="Yes"/>
<DHCP_STATIC_ROUTE value="Yes"/>
<REG_WINS_SERVER value="Yes"/>
<PRIM_DNS_SERVER value="0.0.0.0"/>
<SEC_DNS_SERVER value="0.0.0.0"/>
<TER_DNS_SERVER value="0.0.0.0"/>
<PRIM_WINS_SERVER value="0.0.0.0"/>
<SEC_WINS_SERVER value="0.0.0.0"/>
<STATIC_ROUTE_1 DEST="0.0.0.0" GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_2 DEST="0.0.0.0" GATEWAY="0.0.0.0"/>
<STATIC_ROUTE_3 DEST="0.0.0.0" GATEWAY="0.0.0.0"/>
<!-- This tag can be used on an iLO blade server to force iLO -->
<!-- to attempt to get an IP address from the signal backplane -->
<!-- in a server enclosure. The IP address must be set prior -->
<!-- with Mod_Enc_Bay_IP_Settings.xml -->
<!-- <ENCLOSURE_IP_ENABLE VALUE="Yes"/> -->
</MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>

```

Modify VLAN example:

```

<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="WRITE" >
    <MOD_NETWORK_SETTINGS>
      <SHARED_NETWORK_PORT VALUE="Yes"/>
      <VLAN_ENABLED VALUE="Yes"/>
      <VLAN_ID VALUE="1"/>
    </MOD_NETWORK_SETTINGS>
  </RIB_INFO>
</LOGIN>
</RIBCL>

```

RBSU POST IP example:

```

<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">

```



```

    <RIB_INFO MODE="write" >
    <MOD_GLOBAL_SETTINGS>
        <RBSU_POST_IP VALUE="Y"/>
    </MOD_GLOBAL_SETTINGS>
    </RIB_INFO>
</LOGIN>
</RIBCL>

```

Shared network port example:

```

<RIBCL version="2.21">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="WRITE" >
    <MOD_NETWORK_SETTINGS>
        <!-- Desired NIC: Substitute: -->
        <!-- iLO NIC <SHARED_NETWORK_PORT VALUE="N"/> -->
        <!-- Host NIC <SHARED_NETWORK_PORT VALUE="Y"/ -->
        <SHARED_NETWORK_PORT VALUE="N"/>
    </MOD_NETWORK_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

MOD_NETWORK_SETTINGS parameters

If the following parameters are not specified, then the parameter value for the specified setting is preserved. Zero values are not permitted in some fields. Consequently, an empty string deletes the current value in some fields.

ENABLE_NIC enables the NIC to reflect the state of iLO 2. The values are "Yes" or "No." It is case insensitive.

SHARED_NETWORK_PORT sets the Shared Network Port value. The values are "Yes" or "No." For iLO, the Shared Network Port feature is only available on servers with hardware, NIC firmware, and iLO firmware that supports this feature. For iLO 2, the Shared Network Port is supported on all firmware versions, and the feature is available if the hardware is supported.

ProLiant server	Minimum iLO firmware version
DL320G3	1.64
DL360 G4	1.60
DL360 G4	1.64
DL380 G4	1.60
DL385 G1	1.64
DL580 G3	1.64
ML370 G4	1.60
ML570 G3	1.64

When using the iLO 2 Shared Network Port, flashing the iLO 2 firmware through the XML interface takes approximately 7 minutes to complete. Flashing the firmware using Shared Network Port with iLO 2 does not take any longer to complete than using the dedicated iLO 2 management port.

SHARED_NETWORK_PORT_VLAN VALUE enables iLO 2 Shared Network Port VLAN ID tagging. The possible values are "Yes" or "No."

SHARED_NETWORK_PORT_VLAN_ID VALUE sets the VLAN ID value. Values must be between 1 and 4094.

REG_DDNS_SERVER VALUE instructs iLO 2 to register the management port with a DDNS server. The possible values are "Yes" or "No."

SPEED_AUTOSELECT is a Boolean parameter to enable or disable the iLO 2 transceiver to auto-detect the speed and duplex of the network. This parameter is optional, and the Boolean string must be set to "Yes" if this behavior is desired. If this parameter is used, the Boolean string value must never be left blank. The possible values are "Yes" or "No." It is case insensitive.

FULL_DUPLEX is used to decide if the iLO 2 is to support full-duplex or half-duplex mode. It is only applicable if SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

NIC_SPEED is used to set the transceiver speed if SPEED_AUTOSELECT was set to "No." The possible values are "10" or "100." Any other values will result in a syntax error.

DHCP_ENABLE is used to enable DHCP. The possible values are "Yes" or "No." It is case insensitive.

IP_ADDRESS is used to select the IP address for the iLO 2 if DHCP is not enabled. If an empty string is entered, the current value is deleted.

SUBNET_MASK is used to select the subnet mask for the iLO 2 if DHCP is not enabled. If an empty string is entered, the current value is deleted.

GATEWAY_IP_ADDRESS is used to select the default gateway IP address for the iLO 2 if DHCP is not enabled. If an empty string is entered, the current value is deleted.

DNS_NAME is used to specify the DNS name for the iLO 2. If an empty string is entered, the current value is deleted.

DOMAIN_NAME is used to specify the domain name for the network where the iLO 2 resides. If an empty string is entered, the current value is deleted.

DHCP_GATEWAY specifies if the DHCP-assigned gateway address is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_DNS_SERVER specifies if the DHCP-assigned DNS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_WINS_SERVER specifies if the DHCP-assigned WINS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_STATIC_ROUTE specifies if the DHCP-assigned static routes are to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

REG_WINS_SERVER specifies if the iLO 2 must be register with the WINS server. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

PRIM_DNS_SERVER specifies the IP address of the primary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_DNS_SERVER specifies the IP address of the secondary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

TER_DNS_SERVER specifies the IP address of the tertiary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

PRIM_WINS_SERVER specifies the IP address of the primary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_WINS_SERVER specifies the IP address of the secondary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

STATIC_ROUTE_1, STATIC_ROUTE_2, and STATIC_ROUTE_3 are used to specify the destination and gateway IP addresses of the static routes. The following two parameters are used within the static route commands. If an empty string is entered, the current value is deleted.

- DEST specifies the destination IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.
- GATEWAY specifies the gateway IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

WEB_AGENT_IP_ADDRESS specifies the address for the Web-enabled agents. If an empty string is entered, the current value is deleted.

MOD_NETWORK_SETTINGS runtime errors

The possible MOD_NETWORK_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_GLOBAL_SETTINGS

The GET_GLOBAL_SETTINGS command requests the respective iLO 2 global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_GLOBAL_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_GLOBAL_SETTINGS parameters

None

GET_GLOBAL_SETTINGS runtime errors

None

GET_GLOBAL_SETTINGS return messages

A possible GET_GLOBAL_SETTINGS return message is as follows:

```
<GET_GLOBAL_SETTINGS>
  <SESSION_TIMEOUT="120">
  <ILO_FUNCT_ENABLED VALUE="Y"/>
  <F8_PROMPT_ENABLED="Y"/>
  <F8_LOGIN_REQUIRED="Y"/>
  <REMOTE_CONSOLE_PORT_STATUS VALUE="2"/>
  <REMOTE_CONSOLE_ENCRYPTION VALUE="Y"/>
  <REMOTE_CONSOLE_ACQUIRE VALUE="Y"/>
  <PASSTHROUGH_CONFIG VALUE="3"/>
  <HTTPS_PORT VALUE="443"/>
  <HTTP_PORT VALUE="80"/>
  <REMOTE_CONSOLE_PORT VALUE="23"/>
  <TERMINAL_SERVICES_PORT VALUE="3389"/>
  <VIRTUAL_MEDIA_PORT VALUE="17988"/>
  <MIN_PASSWORD VALUE="8"/>
  <AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
  <REMOTE_KEYBOARD_MODEL VALUE="US"/>
  <SSH_PORT value="22"/>
  <SSH_STATUS value="YES"/>
  <SERIAL_CLI_STATUS value="3"/>
  <SERIAL_CLI_SPEED value="1"/>
</GET_GLOBAL_SETTINGS>
```

A possible GET_GLOBAL_SETTINGS return message from iLO 2 1.30 firmware:

```
<GET_GLOBAL_SETTINGS>
  <SESSION_TIMEOUT VALUE="0"/>
  <ILO_FUNCT_ENABLED VALUE="Y"/>
  <F8_PROMPT_ENABLED VALUE="Y"/>
  <F8_LOGIN_REQUIRED VALUE="N"/>
  <TELNET_ENABLE VALUE="Y"/>
  <PASSTHROUGH_CONFIG VALUE="3"/>
  <HTTPS_PORT VALUE="443"/>
  <HTTP_PORT VALUE="80"/>
  <REMOTE_CONSOLE_PORT VALUE="23"/>
  <TERMINAL_SERVICES_PORT VALUE="3389"/>
  <VIRTUAL_MEDIA_PORT VALUE="17988"/>
  <SSH_PORT VALUE="22"/>
  <CONSOLE_CAPTURE_PORT VALUE="17990"/>
  <SHARED_CONSOLE_PORT VALUE="9300"/>
```

```

<SSH_STATUS VALUE="Y"/>
<SERIAL_CLI_STATUS VALUE="Enabled-Authentication Required"/>
<SERIAL_CLI_SPEED VALUE="9600"/>
<MIN_PASSWORD VALUE="8"/>
<AUTHENTICATION_FAILURE_LOGGING VALUE="Enabled-every 3rd failure"/>
<REMOTE_KEYBOARD_MODEL VALUE="US"/>
<RBSU_POST_IP VALUE="Y"/>
<HIGH_PERFORMANCE_MOUSE VALUE="Enabled"/>
<REMOTE_CONSOLE_ACQUIRE VALUE="Y"/>
<CONSOLE_CAPTURE_ENABLE VALUE="Disabled"/>
<CONSOLE_CAPTURE_BOOT_BUFFER_ENABLE VALUE="Disabled"/>
<CONSOLE_CAPTURE_FAULT_BUFFER_ENABLE VALUE="Disabled"/>
<INTERACTIVE_CONSOLE_REPLAY_ENABLE VALUE="Disabled"/>
<CAPTURE_AUTO_EXPORT_ENABLE VALUE="Disabled"/>
<CAPTURE_AUTO_EXPORT_LOCATION
VALUE="http://192.168.1.1/folder/capture%h%t.ilo"/>
<CAPTURE_AUTO_EXPORT_USERNAME VALUE=""/>
<CAPTURE_AUTO_EXPORT_PASSWORD VALUE=""/>
<SHARED_CONSOLE_ENABLE VALUE="Enabled"/>
<ENFORCE_AES VALUE="N"/>
</GET_GLOBAL_SETTINGS>

```

MOD_GLOBAL_SETTINGS

The MOD_GLOBAL_SETTINGS command modifies global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

The Lights-Out device (not the server) resets automatically to make changes to port settings effective. Setting the ILO_FUNCT_ENABLED to No disables the management functions of iLO 2 and iLO. If disabled, you must use the iLO Security Override Switch on the server system board and the iLO 2/iLO RBSU (F8 key) to re-enable iLO 2/iLO.

Example 1: Use CPQLOCFG.EXE version 2.26 or greater with the following scripts.

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_GLOBAL_SETTINGS>
  <SESSION_TIMEOUT value="60"/>
  <F8_PROMPT_ENABLED value="Yes"/>
  <HTTP_PORT value="80"/>
  <HTTPS_PORT value="443"/>
  <REMOTE_CONSOLE_PORT value="23"/>
  <REMOTE_CONSOLE_PORT_STATUS value="2"/>
<!-- Firmware support information for next 6 tags: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1.50 and later. -->
<!-- RILOE II - None. -->
  <REMOTE_CONSOLE_ENCRYPTION value="Yes"/>

```

```

    <MIN_PASSWORD value="8"/>
    <ILO_FUNCT_ENABLED value="Yes"/>
    <VIRTUAL_MEDIA_PORT value="17988"/>
    <F8_LOGIN_REQUIRED value="No"/>
    <REMOTE_KEYBOARD_MODEL value="US"/>
<!-- Firmware support information for next 2 tags: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1.50 and later. -->
<!-- RILOE II - Version 1.20 and later. -->
    <PASSTHROUGH_CONFIG value="1"/>
    <TERMINAL_SERVICES_PORT value="3389"/>
<!-- Firmware support information for next 5 tags: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1.60 and later. -->
<!-- RILOE II - None. -->
    <SSH_PORT value="22"/>
    <SSH_STATUS value="Yes"/>
    <SERIAL_CLI_STATUS value="3"/>
    <SERIAL_CLI_SPEED value="1"/>
    <RBSU_POST_IP value="Y"/>
<!-- Firmware support information for next tag: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - None. -->
<!-- RILOE II - None. -->
    <TELNET_ENABLE value="yes"/>
<!-- Firmware support information for next tag: -->
<!-- iLO 2 - All versions. -->
<!-- iLO - Version 1.75 and later. -->
<!-- RILOE II - None. -->
<!-- It can have the following three values -->
<!-- Disabled: Value = "No" -->
<!-- the mouse uses "relative" coordinates mode, -->
<!-- compatible with most host operating systems. -->
<!-- Enabled: Value = "Yes" -->
<!-- the mouse uses "absolute" coordinates mode, -->
<!-- eliminating synchronization issues -->
<!-- on supported operating systems -->
<!-- Automatic: Value = "Automatic" -->
<!-- iLO picks the appropriate mouse mode when -->
<!-- the iLO 2 driver is loaded on the host operating system.-->
<!-- The selected mode is persistent unless a different -->
<!-- mode is indicated when the OS driver is loaded or -->
<!-- if you choose another setting. -->
    <HIGH_PERFORMANCE_MOUSE value="Automatic" />
<!-- Firmware support information for next 13 tags: -->
<!-- iLO 2 - Version 1.30 and later. -->
<!-- iLO - None. -->
<!-- RILOE II - None. -->
    <ENFORCE_AES value="Y"/>
    <AUTHENTICATION_FAILURE_LOGGING value="3"/>
    <CONSOLE_CAPTURE_ENABLE value="Yes" />
    <CONSOLE_CAPTURE_BOOT_BUFFER_ENABLE value="Yes" />

```

```

<CONSOLE_CAPTURE_FAULT_BUFFER_ENABLE value="Yes" />
<INTERACTIVE_CONSOLE_REPLAY_ENABLE value="Yes" />
<CONSOLE_CAPTURE_PORT value="17990" />
<CAPTURE_AUTO_EXPORT_ENABLE value="No" />
<CAPTURE_AUTO_EXPORT_LOCATION
value="HTTP://1.1.1.1/folder/capture%h%t.ilo" />
<CAPTURE_AUTO_EXPORT_USERNAME value="username" />
<CAPTURE_AUTO_EXPORT_PASSWORD value="password" />
<SHARED_CONSOLE_ENABLE value="No" />
<SHARED_CONSOLE_PORT value="9300" />
<!-- Firmware support information for next two tags:-->
<!-- iLO 2 - Version 1.75 and later.-->
<!-- iLO - None. -->
<!-- RILOE II - None. -->
    <KEY_UP_KEY_DOWN value="Yes"/>
    <CAPTURE_MANUAL_EXPORT value="Yes"/>
<!-- Firmware support information for next tag: -->
<!-- iLO 2 - Version 1.10 and later. -->
<!-- iLO - Version 1.80 and later. -->
<!-- RILOE II - None. -->
    <REMOTE_CONSOLE_ACQUIRE value="Yes" />
<!-- Firmware support information for next 13 tags: -->
<!-- iLO 2 - None. -->
<!-- iLO - None. -->
<!-- RILOE II - All versions. -->
    <!--
    <HOST_KEYBOARD_ENABLED value = "YES"/>
    <REMOTE_KEYBOARD_MODEL value = "US"/>
    <POCKETPC_ACCESS value = "YES"/>
    <CIPHER_STRENGTH value = "128"/>
    <SNMP_ADDRESS_1 value = "123.124.125.126"/>
    <SNMP_ADDRESS_2 value = "test"/>
    <SNMP_ADDRESS_3 value = "dest"/>
    <OS_TRAPS value = "Y"/>
    <RIB_TRAPS value = "N"/>
    <CIM_SECURITY_MASK value = "3"/>
    <EMS_STATUS value = "Y" />
    <BYPASS_POWER_CABLE_REPORTING value = "N" />
    <SNMP_PASSTHROUGH_STATUS value = "Y" />
    -->
</MOD_GLOBAL_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

As of release iLO 2 version 1.50, the Virtual Serial Port supports automatically enabling and disabling software flow control. By default, this behavior is disabled. You can enable this configuration option using the RIBCL only. To enable this option, execute the following script:

Example 2:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<RIB_INFO MODE="write">
<MOD_GLOBAL_SETTINGS>
    <VSP_SOFTWARE_FLOW_CONTROL value="Yes"/>
</MOD_GLOBAL_SETTINGS>
<RESET_RIB />
</RIB_INFO>
</LOGIN>
</RIBCL>

```

MOD_GLOBAL_SETTINGS parameters

The following parameters are optional. If you do not specify a parameter, then the parameter value for the specified setting is preserved.

SESSION_TIMEOUT determines the maximum session timeout value in minutes. The accepted values are 0, 15, 30, 60, and 120. A value of 0 specifies infinite timeout.

ILO_FUNCT_ENABLED determines if the Lights-Out functionality is enabled or disabled for iLO 2. The possible values are Yes or No. This parameter is case insensitive.

F8_PROMPT_ENABLED determines if the F8 prompt for ROM-based configuration is displayed during POST. The possible values are "Yes" or "No."

F8_LOGIN_REQUIRED determines if login credentials are required to access the RBSU for iLO 2. The possible values are Yes or No.

REMOTE_CONSOLE_PORT_STATUS determines the behavior of remote console service. The possible values include:

- 0—No change
- 1—Disabled (The remote console port is disabled. This prevents remote console and telnet sessions from being used.)
- 2—Automatic (This is the default setting. The remote console port remains closed unless a remote console session is started.)
- 3—Enabled (The remote console port is always enabled. This enables remote console and telnet sessions to be used.)

REMOTE_CONSOLE_ENCRYPTION determines if remote console data encryption is enabled or disabled. The possible values are Yes and No.

REMOTE_CONSOLE_ACQUIRE determines if the remote console acquire operation is enabled or disabled. The possible values are Yes and No.

PASSTHROUGH_CONFIG determines the behavior of a Microsoft® Terminal Services client. The possible values are as follows:

- 0—No change
- 1—Disabled (The Terminal Services feature is disabled.)
- 2—Automatic (The Terminal Services client is launched when remote console is started.)
- 3—Enabled (This is the default setting. The Terminal Services feature is enabled but does not automatically launch when the Remote Console start.)

HTTPS_PORT—Specifies the HTTPS (SSL) port number.

HTTP_PORT—specifies the HTTP port number.

REMOTE_CONSOLE_PORT—Specifies the port used for remote console.

TERMINAL_SERVICES_PORT—Specifies the port used for terminal services.

VIRTUAL_MEDIA_PORT—Specifies the port used for virtual media.

NOTE: If port changes are detected, the iLO 2 management processor will be rebooted to apply the changes after the script has completed successfully.

MIN_PASSWORD—Specifies how many characters are required in all user passwords. The value can be from zero to 39 characters.

AUTHENTICATION_FAILURE_LOGGING—Specifies logging criteria for failed authentications. The possible values include:

- 0—Disabled
- 1—Enabled (records every authentication failure)
- 2—Enabled (records every second authentication failure)
- 3—Enabled (records every third authentication failure: this is the default value.)
- 5—Enabled (records every fifth authentication failure)

REMOTE_KEYBOARD_MODEL—Determines the remote keyboard language translation used during remote console operation. The possible values include:

US	Belgian	British
Danish	Finnish	French
French Canadian	German	Italian
Japanese	Latin American	Portuguese
Spanish	Swedish	Swiss French
Swiss German		

SSH_PORT—Specifies the port used for SSH connection on iLO 2. The processor must be reset if this value is changed.

SSH_STATUS—Determines if SSH is enabled. The valid values are Yes or No, which enable or disable SSH functionality.

SERIAL_CLI_STATUS—Specifies the status of the CLI. The possible values include:

- 0—No change
- 1—Disabled
- 2—Enabled (no authentication required)
- 3—Enabled (authentication required)

SERIAL_CLI_SPEED—Specifies the CLI port speed. The possible values include:

- 0—No change
- 1—9,600 bps
- 2—19,200 bps

- 3—38,400 bps
- 4—57,600 bps
- 5—115,200 bps

ENFORCE_AES—Determines if iLO 2 enforces the use of AES/3DES encryption ciphers over the iLO 2 interface, SSH, and XML connections. The possible values are Yes and No.

VSP_SOFTWARE_FLOW_CONTROL—Specifies if the Virtual Serial Port automatically enables and disables software flow control. The possible values are Yes or No.

MOD_GLOBAL_SETTINGS runtime errors

The possible MOD_GLOBAL_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.
- Unrecognized keyboard model.

GET_SNMP_IM_SETTINGS

The GET_SNMP_IM_SETTINGS command requests the respective iLO 2 SNMP IM settings. For this command to parse correctly, the GET_SNMP_IM_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_SNMP_IM_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_SNMP_IM_SETTINGS parameters

None

GET_SNMP_IM_SETTINGS runtime errors

None

GET_SNMP_IM_SETTINGS return messages

A possible GET_SNMP_IM_SETTINGS return message is:

```
<GET_SNMP_IM_SETTINGS>
  <SNMP_ADDRESS_1 VALUE="192.168.125.121"/>
  <SNMP_ADDRESS_2 VALUE="192.168.125.122"/>
  <SNMP_ADDRESS_3 VALUE="192.168.125.123"/>
  <OS_TRAPS VALUE="Yes"/>
  <RIB_TRAPS VALUE="No"/>
```

```

    <SNMP_PASSTHROUGH_STATUS VALUE="No"/>
    <WEB_AGENT_IP_ADDRESS VALUE="192.168.125.120"/>
    <CIM_SECURITY_MASK VALUE="3"/>
</GET_SNMP_IM_SETTINGS>

```

MOD_SNMP_IM_SETTINGS

MOD_SNMP_IM_SETTINGS is used to modify SNMP and Insight Manager settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <MOD_SNMP_IM_SETTINGS>
        <WEB_AGENT_IP_ADDRESS value="192.168.125.120"/>
        <SNMP_ADDRESS_1 value="192.168.125.121"/>
        <SNMP_ADDRESS_2 value="192.168.125.122"/>
        <SNMP_ADDRESS_3 value="192.168.125.123"/>
        <OS_TRAPS value="Yes"/>
        <RIB_TRAPS value="No"/>
        <SNMP_PASSTHROUGH_STATUS value="No"/>
        <CIM_SECURITY_MASK value="3"/>
      </MOD_SNMP_IM_SETTINGS>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

MOD_SNMP_IM_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

WEB_AGENT_IP_ADDRESS is the address for the Web-enabled agents. The value for this element has a maximum length of 50 characters. It can be any valid IP address. If an empty string is entered, the current value is deleted.

SNMP_ADDRESS_1, SNMP_ADDRESS_2, and SNMP_ADDRESS_3 are the addresses that receive traps sent to the user. Each of these parameters can be any valid IP address and has a maximum value of 50 characters.

OS_TRAPS determines if the user should receive SNMP traps that are generated by the operating system. The possible values are "Yes" and "No." By default, the value is set to "No."

RIB_TRAPS determines if the user should receive SNMP traps that are generated by the RIB. The possible values are "Yes" and "No." By default, the value is set to "No."

SNMP_PASSTHROUGH_STATUS determines if iLO can receive/ send SNMP request from/ to the host OS. By default, the value is set to "Yes."

CIM_SECURITY_MASK accepts an integer between 0 and 4. The possible values are:

- **0**—No change
- **1**—None (No data is returned.)
- **2**—Low (Name and status data are returned. Associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.)
- **3**—Medium (iLO 2 and server associations are present but the summary page contains less detail than at high security.)
- **4**—High (Associations are present and all data is present on the summary page.)

Each value indicates the level of data returned over the HTTP port.

MOD_SNMP_IM_SETTINGS runtime errors

The possible MOD_SNMP_IM_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

UPDATE_RIB_FIRMWARE

The UPDATE_RIB_FIRMWARE command copies a specified file to iLO 2, starts the upgrade process, and reboots the board after the image has been successfully flashed. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example 1:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <!-- Firmware support information for next tag:-->
      <!-- iLO 2 - 1.70 and later. For servers with TPM enabled.-->
      <!-- iLO - None -->
      <!-- Riloe II - None -->
      <TPM_ENABLED VALUE="Yes"/>
      <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\firmware.bin"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

When you send an XML script to update iLO 2 firmware, iLO 2 firmware verifies the TPM configuration status of option ROM measuring. If it is enabled, iLO 2 firmware returns the same warning message as stated in web interface. You can add the TPM_ENABLE command to the script file. HP recommends using XML script syntax to execute firmware updates. To enable the firmware update to continue, you must set TPM_ENABLE to a value of Y or Yes.

Example 2:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <RIB_INFO MODE="write">
      <TPM_ENABLE = "Yes"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

```

        <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\x1170\iLO2_170D.bin"/>
    </RIB_INFO>
</LOGIN>
</RIBCL>

```

UPDATE_RIB_FIRMWARE parameters

IMAGE_LOCATION is the full path file name of the firmware upgrade file.

TPM_ENABLE enables the firmware to continue updating when option ROM measuring is enabled. To enable the firmware update to continue, you must set TPM_ENABLE to a value of Y or Yes.

UPDATE_RIB_FIRMWARE runtime errors

The possible UPDATE_RIB_FIRMWARE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Unable to open the firmware image update file.
- Unable to read the firmware image update file.
- The firmware upgrade file size is too big.
- The firmware image file is not valid.
- A valid firmware image has not been loaded.
- The flash process could not be started.
- IMAGE_LOCATION must not be blank.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_FW_VERSION

The GET_FW_VERSION command requests the respective iLO 2 firmware information. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```

<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
        <RIB_INFO MODE="read">
            <GET_FW_VERSION/>
        </RIB_INFO>
    </LOGIN>
</RIBCL>

```

GET_FW_VERSION parameters

None

GET_FW_VERSION runtime errors

None

GET_FW_VERSION return messages

The following information is returned within the response:

```
<GET_FW_VERSION
  FIRMWARE_VERSION = <firmware version>
  FIRMWARE_DATE = <firmware date>
  MANAGEMENT_PROCESSOR = <management processor type>
/>
```

HOTKEY_CONFIG

The HOTKEY_CONFIG command configures the remote console hot key settings in iLO 2. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Uppercase letters are not supported, and are converted automatically to lowercase. If you use double or single quotes, it must be different from the delimiter. Specifying a blank string removes the current value.

For a complete list of supported hotkeys, see "Supported Hot Keys (on page 103)."

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <HOTKEY_CONFIG>
        <CTRL_T value="CTRL,ALT,ESC"/>
        <CTRL_U value="L_SHIFT,F10,F12"/>
        <CTRL_V value=""/>
        <CTRL_W value=""/>
        <CTRL_X value=""/>
        <CTRL_Y value=""/>
      </HOTKEY_CONFIG>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

HOTKEY_CONFIG parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

CTRL_T specifies settings for the CTRL_T hot key. The settings must be separated by commas. For example, CTRL_T="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_U specifies settings for the CTRL_U hot key. The settings must be separated by commas. For example, CTRL_U="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_V specifies settings for the CTRL_V hot key. The settings must be separated by commas. For example, CTRL_V="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_W specifies settings for the CTRL_W hot key. The settings must be separated by commas. For example, CTRL_W="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_X specifies settings for the CTRL_X hot key. The settings must be separated by commas. For example, CTRL_X="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_Y specifies settings for the CTRL_Y hot key. The settings must be separated by commas. For example, CTRL_Y="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

HOTKEY_CONFIG runtime errors

The possible HOTKEY_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The hot key parameter specified is not valid.
- Invalid number of hot keys. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

Supported hot keys

The Program Remote Console Hot Keys page allows you to define up to 6 different sets of hot keys for use during a Remote Console session. Each hot key represents a combination of up to 5 different keys which are sent to the host machine whenever the hot key is pressed during a Remote Console session. The selected key combination (all keys pressed at the same time) are transmitted in its place. For more information, refer to "Remote Console hot keys." The following table lists keys available to combine in a Remote Console hot key sequence.

ESC	F12	:	o
L_ALT	" " (Space)	<	p
R_ALT	!	>	q
L_SHIFT	#	=	r
R_SHIFT	\$?	s
INS	%	@	t
DEL	&	[u
HOME	~]	v
END	(\	w
PG UP)	^	x
PG DN	*	_	y
ENTER	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	
F2	0	e	;
F3	1	f	'
F4	2	g	L_CTRL
F5	3	h	R_CTRL

F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	SCRL LCK
F9	7	l	BACKSPACE
F10	8	m	SYS RQ
F11	9	n	

LICENSE

The LICENSE command activates or deactivates the iLO's advanced features. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

On a ProLiant BL Class server, there is no need for a licensing key. Advanced features are automatically activated.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
      <LICENSE>
        <ACTIVATE KEY="1111122222333334444455555"/>
      </LICENSE>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

LICENSE parameters

ACTIVATE followed by a valid KEY value signals the activation of the iLO 2 advanced pack licensing.

KEY specifies the license key value. The key should be entered as one continuous string. Commas, periods, or other characters should not separate the key value. The key will only accept 25 characters; other characters entered to separate key values will be interpreted as a part of the key and result in the wrong key being entered.

LICENSE runtime errors

The possible LICENSE error messages include:

- License key error.
- License is already active.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

INSERT_VIRTUAL_MEDIA

This command notifies iLO 2 of the location of a diskette image. The INSERT_VIRTUAL_MEDIA command must display within a RIB_INFO element, and RIB_INFO must be in write mode.

Example:


```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
    <RIB_INFO MODE = "write">
      <INSERT_VIRTUAL_MEDIA DEVICE="FLOPPY" IMAGE_URL=
        "http://servername/path/to/file"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>

```

INSERT_VIRTUAL_MEDIA parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

IMAGE_URL specifies the URL for the diskette image. The URL format is as follows:

protocol://username:password@hostname:port/filename,cgi-helper

- The protocol field is mandatory and must be either http or https.
- The username:password field is optional.
- The hostname field is mandatory.
- The port field is optional.
- The filename field is mandatory.
- The cgi-helper field is optional.

In addition, the filename field can contain tokens that expand to host-specific strings:

- %m expands to the iLO 2 MAC address.
- %i expands to the iLO 2 IP address in dotted-quad form.
- %h expands to the iLO 2 hostname.

Examples:

```

http://john:abc123@imgserver.company.com/disk/win98dos.bin,/cgi-
bin/hpvfhelp.pl
http://imgserver.company.com/disk/boot%m.bin

```

This command specifies only the location of the image to be used. For the image to be connected to the server, the appropriate BOOT_OPTION must be specified using the SET_VM_STATUS command. If BOOT_OPTION is set to BOOT_ONCE and the server is rebooted, any subsequent server reboots eject the image.

INSERT_VIRTUAL_FLOPPY runtime errors

The possible INSERT_VIRTUAL_FLOPPY error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- IMAGE_URL must not be blank.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- Unable to parse Virtual Media URL
- An invalid Virtual Media option has been given.

- Virtual Media already connected through a script. You must eject or disconnect before inserting new media.

EJECT_VIRTUAL_MEDIA

EJECT_VIRTUAL_MEDIA ejects the Virtual Media image if one is inserted. The EJECT_VIRTUAL_MEDIA command must display within a RIB_INFO element and RIB_INFO must be in write mode.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Admin" PASSWORD="Password">
    <RIB_INFO MODE="write">
      <EJECT_VIRTUAL_MEDIA DEVICE="FLOPPY"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

EJECT_VIRTUAL_MEDIA parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

EJECT_VIRTUAL_MEDIA runtime errors

The possible EJECT_VIRTUAL_MEDIA errors are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- No image present in the Virtual Media drive.
- An invalid Virtual Media option has been given.

GET_VM_STATUS

GET_VM_STATUS returns the Virtual Media drive status. This command must display within a RIB_INFO element.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
    <RIB_INFO MODE = "read">
      <GET_VM_STATUS DEVICE="CDROM"/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_VM_STATUS parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

GET_VM_STATUS runtime errors

The possible GET_VM_STATUS error is:

An invalid Virtual Media option has been given.

GET_VM_STATUS return messages

The return message displays the current state of the Virtual Media. The VM_APPLET parameter shows if a virtual media device is already connected via the Virtual Media Applet. If the VM_APPLET = CONNECTED, then the Virtual Media is already in use and cannot be connected via scriptable Virtual Media or Virtual Media XML commands. The DEVICE parameter tells which device this return message is for. The BOOT_OPTION shows the current setting; BOOT_ALWAYS means that the server will always use the Virtual Media device for booting, BOOT_ONCE means that the server will boot to the Virtual Device once and then disconnect the Virtual Media on the subsequent server reboot, and NO_BOOT means that the Virtual Media will not be connected during a server reboot. The WRITE_PROTECT_FLAG parameter shows if the Virtual Media image can be written to. The IMAGE_INSERTED parameter tells if the Virtual Media device is connected via the scriptable Virtual Media or the Virtual Media XML command.

A possible GET_VM_STATUS return message is:

```
VM_APPLET = CONNECTED | DISCONNECTED
DEVICE = FLOPPY | CDROM
BOOT_OPTION = BOOT_ALWAYS | BOOT_ONCE | NO_BOOT
WRITE_PROTECT_FLAG = YES | NO
IMAGE_INSERTED = YES | NO
```

NOTE: If the BOOT_ONCE boot option is selected, all scriptable virtual media parameters are reset to default settings after the server boots. Specifically BOOT_OPTION = NO_BOOT, WRITE_PROTECT = NO, and IMAGE_INSERTED = NO.

SET_VM_STATUS

The SET_VM_STATUS command sets the Virtual Media drive status. This command must appear within a RIB_INFO element, and RIB_INFO must be set to write. All the parameters in the command are optional.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
<RIB_INFO MODE = "write">
  <SET_VM_STATUS DEVICE = "CDROM">
    <VM_BOOT_OPTION value = "BOOT_ONCE"/>
    <VM_WRITE_PROTECT value = "Y"/>
  </SET_VM_STATUS>
</RIB_INFO>
</LOGIN>
</RIBCL>
```

SET_VM_STATUS parameters

DEVICE specifies the Virtual Media device target. The possible values are FLOPPY or CDROM. If the DEVICE is not specified, FLOPPY is assumed. This value is case-sensitive.

VM_BOOT_OPTION specifies the boot option parameter for the Virtual Media. The possible values are BOOT_ALWAYS, BOOT_ONCE, or NO_BOOT. These values control how the Virtual Media device

behaves during the boot phase of the server. Setting these values does not affect the current state of the Virtual Media device. These settings only take effect if the Virtual Media device is connected at server boot.

- **BOOT_ALWAYS** sets the VM_BOOT_OPTION to **BOOT_ALWAYS**. The Virtual Media device will always be connected during server boot. The Virtual Media device is not connected immediately when the VM_BOOT_OPTION is set. The Virtual Media device is connected on the next server boot after setting of the VM_BOOT_OPTION.
- **BOOT_ONCE** sets the VM_BOOT_OPTION to **BOOT_ONCE**. The Virtual Media device is connected during the next server boot, but on any subsequent server boots, it will not be connected. The **BOOT_ONCE** option is intended to boot one time to the Virtual Media device, use that device while the server is running, and then not have the Virtual Media device available on subsequent server reboots. The Virtual Media device is not connected immediately when the VM_BOOT_OPTION is set. The Virtual Media device is connected on the next server boot following the setting of the VM_BOOT_OPTION. After the server has booted once with the Virtual Media device connected, on the subsequent server reboot, the Virtual Media device will not be connected and the following Virtual Media device settings will be reset to their default values:
 - **BOOT_OPTION=NO_BOOT**
 - **IMAGE_INSERTED = NO**
- **NO_BOOT** sets the VM_BOOT_OPTION to **NO_BOOT**. The Virtual Media device is not connected during the next server boot. The Virtual Media device is not disconnected immediately when the VM_BOOT_OPTION is set. The Virtual Media device will be disconnected on the next server boot following the setting of the VM_BOOT_OPTION. After the server has booted, the Virtual Media device will not be connected and the following Virtual Media device settings will be reset to their default values:
 - **BOOT_OPTION = NO_BOOT**
 - **IMAGE_INSERTED = NO**

In addition to the VM_BOOT_OPTIONS, **CONNECT** and **DISCONNECT** are also possible values. The **CONNECT** and **DISCONNECT** settings can be used to control the Virtual Media devices in the same way that they are controlled in the Virtual Media applet. Whenever the **CONNECT** or **DISCONNECT** parameters are set, the Virtual Media device immediately connects or disconnects, respectively, to the server.

- **CONNECT** sets the VM_BOOT_OPTION to **CONNECT**. The Virtual Media device is immediately connected to the server. Setting the VM_BOOT_OPTION to **CONNECT** is equivalent to clicking the device **Connect** button on the Virtual Media Applet. After setting the VM_BOOT_OPTION to **CONNECT**, the VM_GET_STATUS command will show the VM_BOOT_OPTION as **BOOT_ALWAYS**. This is by design and shows that the Virtual Media device is connected like the Virtual Media device in the applet which will always be connected during all server boots.
- **DISCONNECT** sets the VM_BOOT_OPTION to **DISCONNECT**. The Virtual Media device is immediately disconnected from the server. Setting the VM_BOOT_OPTION to **DISCONNECT** is equivalent to clicking the device **Disconnect** button on the Virtual Media Applet. Additionally, setting the VM_BOOT_OPTION to **DISCONNECT** is equivalent to issuing the **EJECT_VIRTUAL_MEDIA** command. When the VM_BOOT_OPTION is set to **DISCONNECT**, the Virtual Media device will not be connected and the following Virtual Media device settings will be reset to their default values:
 - **BOOT_OPTION = NO_BOOT**
 - **IMAGE_INSERTED = NO**

VM_WRITE_PROTECT sets the write protect flag value for the Virtual Floppy. This value is not significant for the Virtual Media CD-ROM. The possible values are Y or N.

SET_VM_STATUS runtime errors

The possible runtime errors are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. VIRTUAL_MEDIA_PRIV required.
- An invalid Virtual Media option has been given.

CERTIFICATE_SIGNING_REQUEST

This command requests a certificate from iLO 2. When this command is received, iLO 2 generates a certificate signing request. The request is returned to the user enclosed in a CERTIFICATE_SIGNING_REQUEST tag. This command requires CPQLOCFG version 2.26 or later.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
    <RIB_INFO MODE = "write">
      <CERTIFICATE_SIGNING_REQUEST/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

CERTIFICATE_SIGNING_REQUEST parameters

There are no parameters for this command.

CERTIFICATE_SIGNING_REQUEST errors

There are no errors for this command.

IMPORT_CERTIFICATE

The IMPORT_CERTIFICATE command imports a signed certificate into iLO 2. The signed certificate must be a signed version of a certificate signing request. This command requires CPQLOCFG version 2.26 or later.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN = "adminname" PASSWORD = "password">
  <RIB_INFO MODE = "write">
    <IMPORT_CERTIFICATE>
      -----BEGIN CERTIFICATE-----
      ...
      -----END CERTIFICATE-----
    </IMPORT_CERTIFICATE>
  </RIB_INFO>
```

```
</LOGIN>
</RIBCL>
```

IMPORT_CERTIFICATE parameters

There are no parameters for this command.

IMPORT_CERTIFICATE errors

The possible IMPORT_CERTIFICATE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Error reading certificate: The imported certificate is invalid.
- Invalid certificate common name: The common name in the certificate does not match iLO 2's hostname.
- Certificate signature does not match private key: The certificate does not correspond to the private key stored in iLO 2.

GET_TWOFACTOR_SETTINGS

The GET_TWOFACTOR_SETTINGS command requests the respective iLO 2 Two-Factor Authentication settings. For this command to parse correctly, the GET_TWOFACTOR_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
      <GET_TWOFACTOR_SETTINGS/>
    </RIB_INFO>
  </LOGIN>
</RIBCL>
```

GET_TWOFACTOR_SETTINGS parameters

None

GET_TWOFACTOR_SETTINGS runtime errors

None

GET_TWOFACTOR_SETTINGS return messages

Starting with iLO 2 1.20, users can be authenticated with a digital certificate. Depending on the iLO 2 Two-Factor Authentication settings, the response to GET_TWOFACTOR_SETTINGS will contain different data.

Examples of GET_TWOFACTOR_SETTINGS return messages are:

Example of a Two-Factor Authentication settings return message with default settings:

```
<GET_TWOFACTOR_SETTINGS>
  <AUTH_TWOFACTOR_ENABLE VALUE="N"/>
```

```

    <CERT_REVOCATION_CHECK VALUE="N"/>
    <CERT_OWNER_SUBJECT/>
  </GET_TWOFACOR_SETTINGS>

```

Example of a Two-Factor Authentication settings return message when SAN field in the certificate for directory authentication is enabled:

```

<GET_TWOFACOR_SETTINGS>
  <AUTH_TWOFACOR_ENABLE VALUE="Y"/>
  <CERT_REVOCATION_CHECK VALUE="N"/>
  <CERT_OWNER_SAN/>
</GET_TWOFACOR_SETTINGS>

```

MOD_TWOFACOR_SETTINGS

The MOD_TWOFACOR_SETTINGS command is used to modify the Two-Factor Authentication settings on the iLO 2. For this command to parse correctly, the MOD_TWOFACOR_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. You must have the configure RLOE II privilege to execute this command. Changing the value of AUTH_TWOFACOR_ENABLE will cause the iLO 2 to reset for the new setting to take effect.

NOTE: The GET_TWOFACOR_SETTINGS and MOD_TWOFACOR_SETTINGS commands are supported with iLO firmware version 1.80 and above and with iLO 2 firmware version 1.10 and above. iLO 1.80 requires CPQLOCFG version 2.24, and iLO 1.10 requires CPQLOCFG version 2.25.

A Trusted CA Certificate is required for Two-Factor Authentication to function. The iLO 2 will not allow the AUTH_TWOFACOR_ENABLE setting to be set to Yes if a Trusted CA certificate has not been configured. Also, a client certificate must be mapped to a local user account if local user accounts are being used. If the iLO 2 is using directory authentication, client certificate mapping to local user accounts is optional.

To provide the necessary security, the following configuration changes are made when Two-Factor Authentication is enabled:

- Remote Console Data Encryption: Yes (this will disable telnet access)
- Enable Secure Shell (SSH) Access: No
- Serial Command Line Interface Status: Disabled

If telnet, SSH or Serial CLI access is required, re-enable these settings after Two-Factor Authentication is enabled. However, because these access methods do not provide a means of Two-Factor Authentication, only a single factor is required to access the iLO 2 with telnet, SSH, or serial CLI.

When Two-Factor Authentication is enabled, access with the CPQLOCFG utility is disabled because CPQLOCFG does not supply all authentication requirements. However, the HPONCFG utility is functional, since administrator privileges on the host system are required to execute this utility.

- Example of enabling Two-Factor Authentication:


```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
  <MOD_TWOFACOR_SETTINGS>
    <AUTH_TWOFACOR_ENABLE value="Yes"/>
    <CERT_REVOCATION_CHECK value="No"/>

```

```

    <CERT_OWNER_SAN/>
  </MOD_TWOFACOR_SETTINGS>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

- Importing a CA and a user certificate example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="test" PASSWORD="password">
  <RIB_INFO MODE="write">
    <MOD_TWOFACOR_SETTINGS>
      <CERT_OWNER_SAN/>
      <IMPORT_CA_CERTIFICATE>
-----BEGIN CERTIFICATE-----
MIIETzCCA5+gAwIBAgIQBGg9C0d7B5pF/14bVA44hjANBgkqhkiG9w0BAQUFADBMMRMwEQYKZCZImiZPyLGBGRYDTEFCMRUwEwYKZCZImiZPyLGBGRYFSkpSSUIxHjAc
...
9gVCPsOQUGMMZUeNYObkTE0e+MrPGL+TqQEYIakF3rjA2PbL1uSY6d4dLCx7izkO
buEpHTPDqs9gZ3U5ht9bjES93UHnDENLopkZ2JgGwH8Y50eBnjq4xml9psbYZn5Y
yWpONE/IjIjJyww=
-----END CERTIFICATE-----
      </IMPORT_CA_CERTIFICATE>
      <IMPORT_USER_CERTIFICATE USER_LOGIN="apollo">
-----BEGIN CERTIFICATE-----
CZImiZPyLGBGRYDTEFCMRUwEwYKZCZImiZPyLGBGRYFSkpSSUIxHjAcBgNVBAMT
ODU5NDRaMFYxEzARBgoJkiaJk
...
sjbbpNGpxGsK9Gzi5j6UeOYklePyau0TJ3KIm2RPlR2C6XAGz2PTWgsxG1UP9lNH
bfz0+TD0JsschjqK23/vr2GxQ9C/835zRxdu5Dn8JGm3/dFHR2VxgCetIxyR9TQC
ZKTfvIa8N9KvMLZdc1Sj94jUyMZjYYmCWULW8WySMV70nclvrsI2hi3nwMtt2Zvj
WnbeZujBX9LGz3HdmghgUw4GTwYl3ZG88snuTyXliLPFXVYXvNAhGeWqXtrh7A90
3NprjG7DM1uw
-----END CERTIFICATE-----
      </IMPORT_USER_CERTIFICATE>
    </MOD_TWOFACOR_SETTINGS>
  </RIB_INFO>
</LOGIN>
</RIBCL>

```

MOD_TWOFACOR_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

AUTH_TWOFACOR_ENABLE enables or disables Two-Factor authentication. The possible values are "Yes" and "No."

CERT_REVOCATION_CHECK causes iLO 2 to use the CRL distribution point attribute of the client certificate to download the CRL and check against revocation. The possible values are "Yes" and "No." If this setting is set to Yes, and the CRL cannot be downloaded for any reason, authentication will be denied.

CERT_OWNER_SAN causes iLO 2 to extract the User Principle Name from the Subject Alternative Name, and use that for authentication with the directory, for example: username@domain.extension.

CERT_OWNER_SUBJECT causes iLO 2 to derive the user's distinguished name from the subject name. For example, if the subject name is "/DC=com/DC=domain/OU=organization/CN=user," iLO 2 will derive: "CN=user,OU=organization,DC=domain,DC=com."

The CERT_OWNER_SAN and CERT_OWNER_SUBJECT settings are only used if directory authentication is enabled.

IMPORT_CA_CERTIFICATE imports the certificate into iLO 2 as the trusted Certificate Authority. iLO 2 will only allow client certificates that are issued by this CA. A Trusted CA certificate must be configured in iLO 2 for Two-Factor authentication to function.

IMPORT_USER_CERTIFICATE imports the certificate into iLO 2 and maps it to the specified local user. Any client that authenticates with this certificate will authenticate as the local user to which it is mapped. The SHA1 hash of this certificate will be displayed on the Modify User website for the user to whom it is mapped. If iLO 2 is using directory authentication, client certificate mapping to local user accounts is optional and only necessary if authentication with local accounts is desired.

The IMPORT_CA_CERTIFICATE and IMPORT_USER_CERTIFICATE settings require that base64-encoded certificate data be included between the BEGIN and END tags.

MOD_TWOFACOR_SETTINGS runtime errors

The possible MOD_TWOFACOR_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- This setting cannot be changed while Shared Network port is enabled.
iLO 2 has been configured to use shared network port, which will not function if Two-factor authentication is enabled
- This setting cannot be enabled unless a trusted CA certificate has been imported.
A CA certificate must be imported before enabling Two-factor authentication.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

DIR_INFO

The DIR_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local directory information database into memory and prepares to edit it. Only commands that are DIR_INFO type commands are valid inside the DIR_INFO command block. The DIR_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

DIR_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO 2 information. Read mode prevents modification of the iLO 2 information.

Example:

```
<DIR_INFO MODE="read">
..... DIR_INFO commands .....
</DIR_INFO>
```

GET_DIR_CONFIG

The GET_DIR_CONFIG command requests the respective iLO 2 directory settings. For this command to parse correctly, the GET_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <DIR_INFO MODE="read">
      <GET_DIR_CONFIG/>
    </DIR_INFO>
  </LOGIN>
</RIBCL>
```

GET_DIR_CONFIG parameters

None

GET_DIR_CONFIG runtime errors

None

GET_DIR_CONFIG return messages

Starting with iLO 2 1.80, directory integration can work with HP Lights-Out schema with or without extensions (schema-free). Depending on your directory configuration, the response to GET_DIR_CONFIG contains different data.

Possible GET_DIR_CONFIG return messages are:

- Example of a directory services (with schema extension) return message:

```
<GET_DIR_CONFIG>
  <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
  <DIR_LOCAL_USER_ACCT VALUE="Y"/>
  <DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
  <DIR_SERVER_PORT VALUE="636"/>
  <DIR_OBJECT_DN VALUE="CN=SERVER1_RIB,OU=RIB,DC=HPRIB, DC=LABS"/>
  <DIR_USER_CONTEXT1 VALUE="CN=Users0,DC=HPRIB0, DC=LABS"/>
  <DIR_USER_CONTEXT2 VALUE="CN=Users1,DC=HPRIB1, DC=LABS"/>
  <DIR_USER_CONTEXT3 VALUE=""/>
  <DIR_ENABLE_GRP_ACCT VALUE="N"/>
</GET_DIR_CONFIG>
```

- Example of a schema-free directory (without schema extension) return message:

```
<GET_DIR_CONFIG>
  <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
  <DIR_LOCAL_USER_ACCT VALUE="Y"/>
  <DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
  <DIR_SERVER_PORT VALUE="636"/>
```

```

<DIR_OBJECT_DN VALUE="" />
<DIR_USER_CONTEXT1 VALUE="CN=Users,DC=demo,DC=com" />
<DIR_USER_CONTEXT2 VALUE="" />
<DIR_USER_CONTEXT3 VALUE="" />
<DIR_ENABLE_GRP_ACCT VALUE="Y" />
<DIR_GRPACCT1_NAME VALUE="CN=iLOAdmins,CN=Users,DC=demo,DC=com" />
<DIR_GRPACCT1_PRIV VALUE="1,2,3,4,5" />
<DIR_GRPACCT2_NAME VALUE="" />
<DIR_GRPACCT2_PRIV VALUE="" />
<DIR_GRPACCT3_NAME VALUE="" />
<DIR_GRPACCT3_PRIV VALUE="" />
<DIR_GRPACCT4_NAME VALUE="" />
<DIR_GRPACCT4_PRIV VALUE="" />
<DIR_GRPACCT5_NAME VALUE="" />
<DIR_GRPACCT5_PRIV VALUE="" />
<DIR_GRPACCT6_NAME VALUE="" />
<DIR_GRPACCT6_PRIV VALUE="" />
</GET_DIR_CONFIG><GET_DIR_CONFIG>

```

IMPORT_SSH_KEY

The IMPORT_SSH_KEY command imports a SSH_KEY and associated iLO 2 user name into iLO 2. This command requires CPQLOCFG version 2.27 or later.

After generating an SSH key using `ssh-keygen` and creating the `key.pub` file, you must perform the following:

1. Locate the `key.pub` file and insert its contents between "-----BEGIN SSH KEY-----" and "-----END SSH KEY-----". The file begins with the text `ssh-dss` or `ssh-rsa`.
2. At the end of the key, append a space and the name of a valid iLO 2 user name as displayed on the Modify User page. For example: `xxx_some text_xxx ASmith`.

The user name is case-sensitive and must match the case of the iLO 2 user name to associate the SSH key with the correct user.

Example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <RIB_INFO MODE="write">
    <IMPORT_SSH_KEY>
      -----BEGIN SSH KEY-----

      ssh-dss
      ContentOfYourSSHKeyBALftnNE12JR8T8XQqyzqc1tt6FLFRXLRM5PJpOf/IG4hN45
      +x+JbaqkhH+aKqFjlf01NjszHrFN26H1AhW0jY2bEwj2w1JzBMAhXwnPQelQsCnJDf+
      zCzbDn+5Va86+qWxm0lsDEChvZPM6wpjkXvHwuInjxTzOGQTq++vmYlo1/AAAAFQC1M
      FaZjE995QhX9H1DaDzpsVTXvwAAAIA6ec/hAkas2N762jtlHvSuvZaQRzu49D0tjXVI
      pNdJAhtC8O2505PzkGLf5qhrbDnusc1CvoH7DuxyHjeOUVxbC5wFQBcGF4VnpYZ8nGQ
      Gt9TQ0iUV+NRwn4CR5ESoi63zTJIvKIYZDT2ISeXhF2iU6txjZzdeEm7vQz3slaY3dg
      AAAIAQ46i6FBzJAYXziF/qmWMt4y6SlylOQDAsxPKk7rpxegv8RlTeon/aeL7objb9GQ
      2xnEN5gobANZxKz2d4/jwg3+qgTDT6V1G+b7+nEI/XHic717/7oqgiOv4VE3WxN+HE9
      JWsv2jwUpAzRGqJOoojRG/CCru0K+jgTOF/dilo0sw== ASmith
    
```

```

-----END SSH KEY-----
</IMPORT_SSH_KEY>
</RIB_INFO>
</LOGIN>
</RIBCL>

```

IMPORT_SSH_KEY parameters

There are no parameters for this command.

IMPORT_SSH_KEY runtime errors

The possible IMPORT_SSH_KEY error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Error reading SSH Key: The imported SSH Key is invalid.
- Invalid iLO user name: The appended user name is not a valid iLO 2 user.
- No slots are available for storing additional SSH Key.

MOD_DIR_CONFIG

The MOD_DIR_CONFIG command modifies the directory settings on iLO 2. For this command to parse correctly, the MOD_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
<DIR_INFO MODE="write">
<MOD_DIR_CONFIG>
    <DIR_AUTHENTICATION_ENABLED value="Yes"/>
    <DIR_LOCAL_USER_ACCT value="Yes"/>
    <!-- For schemaless Directory configuration, ensure that the following
    settings are modified as required so that user can logon with Email
    format and Netbios formats successfully:-->
    <!-- 1. DIR_SERVER_ADDRESS value need to be set to directory server DNS
    Name or FQDN(Full qualified Domain Name)-->
    <!-- Please check and update the following iLO Network Settings. -->
    <!-- 1.The domain name of iLO should match the domain of the directory
    server. -->
    <!-- 2.One of the primary, secondary or tertiary DNS server must have
    the same IP address as the Directory server. -->
    <DIR_SERVER_ADDRESS value="dlilo1.mycompu.com"/>
    <DIR_SERVER_PORT value="636"/>
    <DIR_OBJECT_DN value="CN=server1_rib,OU=RIB, DC=mycompu,DC=com"/>
    <DIR_OBJECT_PASSWORD value="password"/>
    <DIR_USER_CONTEXT_1 value="CN=Users,DC=mycompu, DC=com"/>
    <DIR_USER_CONTEXT_2 value="CN=Users2,DC=mycompu, DC=com"/>
    <DIR_USER_CONTEXT_3 value="CN=Users3,DC=mycompu, DC=com"/>
    <!-- Firmware support information for next 12 tags -->

```

```

<!-- iLO2 1.75 and later -->
<!-- iLO - None -->
<!-- Riloe II - None -->
  <DIR_USER_CONTEXT_4 value="CN=Users4,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_5 value="CN=Users5,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_6 value="CN=Users6,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_7 value="CN=Users7,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_8 value="CN=Users8,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_9 value="CN=Users9,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_10 value="CN=Users10,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_11 value="CN=Users11,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_12 value="CN=Users12,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_13 value="CN=Users13,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_14 value="CN=Users14,DC=mycompu, DC=com"/>
  <DIR_USER_CONTEXT_15 value="CN=Users15,DC=mycompu, DC=com"/>
<!-- Set the value to "NO" to enable the HP Extended Schema -->
<!-- and Value "YES" to enable Default Directory Login. -->
<!-- To set Group Accounts and privileges for Default Schema -->
<!-- run Mod_Schemaless_Directory.xml. -->
  <DIR_ENABLE_GRP_ACCT value = "yes"/>
</MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>

```

NOTE: When using directory integration with schema extension, the following tags must not be used:

- DIR_ENABLE_GRP_ACCT
 - DIR_GRPACCT1_NAME
 - DIR_GRPACCT1_PRIV
-

NOTE: When using schema-free directories, the following tags must not be used:

- DIR_OBJECT_DN
 - DIR_OBJECT_PASSWORD
-

MOD_DIR_CONFIG parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DIR_AUTHENTICATION_ENABLED enables or disables directory authentication. The possible values are Yes and No.

DIR_ENABLE_GRP_ACCT causes iLO 2 to use schema-less directory integration. The possible values are Yes and No.

When using schema-free directory integration, iLO 2 supports variable privileges associated with different directory groups. These groups are contained in the directory, and the corresponding member iLO 2 privileges are stored in iLO 2.

- DIR_GRPACCT1_NAME identifies a group container in the directory, such as Administrators, Users, or Power Users.
- DIR_GRPACCT1_PRIV numerically identify iLO 2 privileges for members of the group. You can mix and match privileges by including more than one value. These privileges are expressed as a comma separated list of numbers (1,2,3,4,5) which correlate to:
 1. Administer Group Accounts
 2. Remote Console Access
 3. Virtual Power and Reset
 4. Virtual Media
 5. Configure iLO 2 Settings

NOTE: When using directory integration with schema extension, the following tags must not be used:

- DIR_ENABLE_GRP_ACCT
 - DIR_GRPACCT1_NAME
 - DIR_GRPACCT1_PRIV
-

NOTE: When using schema-free directories, the following tags must not be used:

- DIR_OBJECT_DN
 - DIR_OBJECT_PASSWORD
-

DIR_LOCAL_USER_ACCT enables or disables local user accounts. The possible values are Yes and No.

DIR_SERVER_ADDRESS specifies the location of the directory server. The directory server location is specified as an IP address or DNS name.

DIR_SERVER_PORT specifies the port number used to connect to the directory server. This value is obtained from the directory administrator. The secure LDAP port is 636, but the directory server can be configured for a different port number.

DIR_OBJECT_DN specifies the unique name of iLO 2 in the directory server. This value is obtained from the directory administrator. Distinguished names are limited to 256 characters.

DIR_OBJECT_PASSWORD specifies the password associated with the iLO 2 object in the directory server. Passwords are limited to 39 characters.

DIR_USER_CONTEXT_1, DIR_USER_CONTEXT_2, and DIR_USER_CONTEXT_3 specify searchable contexts used to locate the user when the user is trying to authenticate using directories. If the user could not be located using the first path, then the parameters specified in the second and third paths are used. The values for these parameters are obtained from the directory administrator. Directory User Contexts are limited to 128 characters each.

MOD_DIR_CONFIG runtime errors

The possible MOD_DIR_CONFIG error messages include:

- Directory information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

RACK_INFO

The RACK_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the rack infrastructure database into memory and prepares to edit it. Only commands that are RACK_INFO type commands are valid inside the RACK_INFO command block. The RACK_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

This command block is only valid on ProLiant BL Class servers. RACK_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO 2 information. Read mode prevents modification of the iLO 2 information.

The possible RACK_INFO error messages include:

- Invalid Mode.
- Server is not a rack server; rack commands do not apply.

Example:

```
<RACK_INFO MODE="read">
..... RACK_INFO commands .....
</RACK_INFO>
```

GET_RACK_SETTINGS

The GET_RACK_SETTINGS command requests the respective iLO 2's rack settings. For this command to parse correctly, the GET_RACK_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RACK_INFO MODE="read">
      <GET_RACK_SETTINGS/>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

GET_RACK_SETTINGS parameters

None

GET_RACK_SETTINGS runtime errors

None

GET_RACK_SETTINGS return messages

A possible GET_RACK_SETTINGS return message is:

```
<GET_RACK_SETTINGS>
  <RACK_NAME VALUE="HPspace"/>
```

```

    <ENCLOSURE_NAME VALUE="Home"/>
    <ENCLOSURE_SN VALUE="44XP0606XP33"/>
    <BAY_NAME VALUE="Library"/>
    <BAY VALUE="2"/>
    <FACILITY_PWR_SOURCE VALUE="N"/>
    <RACK_AUTO_PWR VALUE="Y"/>
    <SNMP_RACK_ALERTS VALUE="Y"/>
    <LOG_RACK_ALERTS VALUE="N"/>
  </GET_RACK_SETTINGS >

```

GET_DIAGPORT_SETTINGS

The GET_DIAGPORT_SETTINGS command requests the respective iLO diagnostic port settings. For this command to parse correctly, the GET_DIAGPORT_SETTINGS command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```

<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RACK_INFO MODE="read">
      <GET_DIAGPORT_SETTINGS/>
    </RACK_INFO>
  </LOGIN>
</RIBCL>

```

GET_DIAGPORT_SETTINGS parameters

None

GET_DIAGPORT_SETTINGS runtime errors

None

GET_DIAGPORT_SETTINGS return messages

A possible GET_DIAGPORT_SETTINGS return message is:

```

<GET_DIAGPORT_SETTINGS>
  <DP_SPEED_AUTOSELECT value="No"/>
  <DP_NIC_SPEED value="100"/>
  <DP_FULL_DUPLEX value="Yes"/>
  <DP_IP_ADDRESS value="192.168.142.56"/>
  <DP_SUBNET_MASK value="255.255.0.0"/>
</GET_DIAGPORT_SETTINGS >

```

MOD_DIAGPORT_SETTINGS

The MOD_DIAGPORT_SETTINGS command is used modify the diagnostic port network settings on iLO 2. For this command to parse correctly, the MOD_DIAGPORT_SETTINGS command must appear within a

RACK_INFO command block, and RACK_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="username" PASSWORD="password">
    <RACK_INFO MODE="write">
      <MOD_DIAGPORT_SETTINGS>
        <DP_SPEED_AUTOSELECT value="No"/>
        <DP_NIC_SPEED value="100"/>
        <DP_FULL_DUPLEX value="Yes"/>
        <DP_IP_ADDRESS value="192.168.142.56"/>
        <DP_SUBNET_MASK value="255.255.0.0"/>
      </MOD_DIAGPORT_SETTINGS>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

MOD_DIAGPORT_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DP_SPEED_AUTOSELECT is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

DP_NIC_SPEED is used to set the transceiver speed if DP_SPEED_AUTOSELECT was set to "No." The possible values are 10 or 100. Any other value results in a syntax error.

DP_FULL_DUPLEX is used to decide if the iLO 2 diagnostic port is to support full-duplex or half-duplex mode. It is only applicable if DP_SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

DP_IP_ADDRESS is used to select the IP address for the iLO 2 Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is XXX.XXX.XXX.XXX.

DP_SUBNET_MASK is used to select the subnet mask for the iLO 2 Diagnostic Port. If an empty string is entered, the current address is unchanged. The expected format is XXX.XXX.XXX.XXX.

The iLO 2 management processor will be rebooted to apply the changes after the script has completed successfully.

MOD_DIAGPORT_SETTINGS runtime errors

Possible MOD_DIAGPORT_SETTINGS error messages include:

- iLO 2 information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_ENCLOSURE_IP_SETTINGS

GET_ENCLOSURE_IP_SETTINGS requests iLO 2 Static IP Bay Configuration settings. This attribute must appear inside the RACK_INFO command block. The RACK_INFO command block can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="Admin" PASSWORD="password">
    <RACK_INFO MODE="write">
      <GET_ENCLOSURE_IP_SETTINGS/>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

GET_ENCLOSURE_IP_SETTINGS parameters

None

GET_ENCLOSURE_IP_SETTINGS return messages

A possible GET_ENCLOSURE_IP_SETTINGS return message is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
  <RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
  />
  <GET_ENCLOSURE_IP_SETTINGS>
    <BAY_ENABLE MASK="0x0002"/>
    <IP_ADDRESS VALUE="170.100.12.101"/>
    <SUBNET_MASK VALUE="255.255.255.0"/>
    <GATEWAY_IP_ADDRESS VALUE="170.100.12.254"/>
    <DOMAIN_NAME VALUE=""/>
    <PRIM_DNS_SERVER VALUE="0.0.0.0"/>
    <SEC_DNS_SERVER VALUE="0.0.0.0"/>
    <TER_DNS_SERVER VALUE="0.0.0.0"/>
    <PRIM_WINS_SERVER VALUE="0.0.0.0"/>
    <SEC_WINS_SERVER VALUE="0.0.0.0"/>
    <STATIC_ROUTE_1 DESTINATION="0.0.0.0"
      GATEWAY="0.0.0.0"/>
    <STATIC_ROUTE_2 DESTINATION="0.0.0.0"
      GATEWAY="0.0.0.0"/>
    <STATIC_ROUTE_3 DESTINATION="0.0.0.0"
      GATEWAY="0.0.0.0"/>
  </GET_ENCLOSURE_IP_SETTINGS>
</RIBCL>
```

MOD_ENCLOSURE_IP_SETTINGS

MOD_ENCLOSURE_IP_SETTINGS modifies the Static IP Bay Configuration settings. This command is only valid inside a RACK_INFO block. The logged-in user must have the configure iLO 2 privilege. This attribute must appear inside the RACK_INFO command block. The RACK_INFO command block can be set to write.

Modify settings example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
<RACK_INFO MODE="write">
  <MOD_ENCLOSURE_IP_SETTINGS>
    <BAY_ENABLE MASK="0x3FE"/>
    <IP_ADDRESS VALUE="16.100.222.111"/>
    <SUBNET_MASK VALUE="255.255.252.0"/>
    <GATEWAY_IP_ADDRESS VALUE="16.100.222.1"/>
    <DOMAIN_NAME VALUE="sum.won.here.now"/>
    <PRIM_DNS_SERVER VALUE="16.11.1.111"/>
    <SEC_DNS_SERVER VALUE=""/>
    <TER_DNS_SERVER VALUE=""/>
    <PRIM_WINS_SERVER VALUE="16.22.2.222"/>
    <SEC_WINS_SERVER VALUE=""/>
    <STATIC_ROUTE_1 DEST="16.33.3.33"
      GATEWAY="16.100.11.11"/>
    <STATIC_ROUTE_2 DEST="" GATEWAY=""/>
    <STATIC_ROUTE_3 DEST="" GATEWAY=""/>
  </MOD_ENCLOSURE_IP_SETTINGS>
</RACK_INFO>
</LOGIN>
</RIBCL>
```

Modify network settings to enable static IP bay configuration example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Admin" PASSWORD="password">
  <RIB_INFO MODE="write">
    <MOD_NETWORK_SETTINGS>
      <ENCLOSURE_IP_ENABLE VALUE="Yes"/>
    </MOD_NETWORK_SETTINGS>
  </RIB_INFO>
</LOGIN>
</RIBCL>
```

MOD_ENCLOSURE_IP_SETTINGS parameters

BAY_ENABLEMASK enables the use of Static IP Bay Configuration addressing. The attribute MASK is a 16-bit number. Each bit represents a slot in the enclosure. If the bit is set, that particular slot is assigned to use the Static IP Bay Configuration settings. The LSB represents slot 1. For example, the MASK="0x0001" only allows slot 1 to use Static IP Bay Configuration. This number can be either a hexadecimal number or a decimal number. This command must appear inside the MOD_ENCLOSURE_IP_SETTINGS block.

ENCLOSURE_IP_ENABLE enables or disables the use of Static IP Bay Configuration. This attribute must appear inside the MOD_NETWORK_SETTINGS command block. The possible values are "Y" or "N." It is case insensitive. This attribute is only applicable on blade servers.

MOD_ENCLOSURE_IP_SETTINGS runtime errors

The possible MOD_ENCLOSURE_IP_SETTINGS error messages include:

- Rack information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV is required.

GET_TOPOLOGY

The GET_TOPOLOGY command requests the respective iLO 2 to return the current topology of the rack infrastructure. For this command to parse correctly, the GET_TOPOLOGY command must appear within a RACK_INFO command block, and RACK_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RACK_INFO MODE="read">
      <GET_TOPOLOGY/>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

GET_TOPOLOGY parameters

None

GET_TOPOLOGY return message

An example of a successful request follows:

```
<RK_TPLGY CNT="3">
<RUID>xxxxxx</RUID>
<ICMB ADDR="0xAA55" MFG="232" PROD_ID="NNN" SER="123" NAME="Power_1">
<LEFT/>
<RIGHT ADDR="0xAB66" SER="123" NAME="Server_1"/>
</ICMB>
<ICMB ADDR="0xAB66" MFG="232" PROD_ID="NNN" SER="456" NAME="Server_1">
<LEFT ADDR="0xAA55" SER="123" NAME="Power_1"/>
<RIGHT ADDR="0xAC77" SER="123" NAME="Power_2"/>
</ICMB>
<ICMB ADDR="0xAC77" MFG="232" PROD_ID="NNN" SER="789" NAME="Power_2">
<RIGHT/>
</ICMB>
</RK_TPLGY>
```

MOD_BLADE_RACK

MOD_BLADE_RACK command is used to modify the rack infrastructure settings. For this command to parse properly, the MOD_BLADE_RACK command must appear within a RACK_INFO command block,

and RACK_INFO MODE must be set to write. The user must have the configure iLO 2 privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RACK_INFO MODE="write">
      <MOD_BLADE_RACK>
        <RACK_NAME value="CPQ_Rack_1"/>
        <ENCLOSURE_NAME value="CPQ_Enclosure_1"/>
        <BAY_NAME value="CPQ_Bay_5"/>
        <FACILITY_PWR_SOURCE value="Yes"/>
        <RACK_AUTO_PWR value="Yes"/>
        <SNMP_RACK_ALERTS value="Yes"/>
        <LOG_RACK_ALERTS value="Yes"/>
      </MOD_BLADE_RACK>
    </RACK_INFO>
  </LOGIN>
</RIBCL>
```

MOD_BLADE_RACK parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

RACK_NAME is the name used to logically group together enclosures in a single rack infrastructure. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

ENCLOSURE_NAME is the name used to logically group together the ProLiant BL-Class servers that compose a single enclosure. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

BAY_NAME is the name used to identify a particular ProLiant BL-Class server. This parameter can be a combination of any printable characters up to a maximum length of 31 characters.

FACILITY_PWR_SOURCE determines the source of power for the blade servers. A value of "Yes" directs the server to use facility power and a value of "No" directs the server to use the server blade power supplies.

RACK_AUTO_PWR determines if the blade server should automatically power when inserted into the enclosure. A value of "Yes" causes the blade server to automatically power up and begin normal booting process if power is available. A value of "No" requires the blade server to be manually powered on.

SNMP_RACK_ALERTS determines if alerts from the rack infrastructure should be forwarded to user-defined SNMP trap destinations. A value of "Yes" enables rack alerts to be forwarded. A value of "No" disables rack alerts from being forwarded.

LOG_RACK_ALERTS determines if alerts from the rack infrastructure should be logged. A value of "Yes" enables rack alerts to be logged in the IML log. A value of "No" disables the logging of rack alerts in the IML log.

MOD_BLADE_RACK runtime errors

The possible MOD_BLADE_RACK error messages include:

- Rack information is open for read-only access. Write access is required for this operation.
- Rack Name too long.
- Enclosure Name too long.
- Bay Name too long.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

SERVER_INFO

The SERVER_INFO command can only appear within a LOGIN command block. Only commands that are SERVER_INFO type commands are valid inside the SERVER_INFO command block.

SERVER_INFO requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO 2 information. Read mode prevents modification of the iLO 2 information.

Example:

```
<SERVER_INFO MODE="read">
..... SERVER_INFO commands .....
</SERVER_INFO>
```

Reset server example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="write">
    <RESET_SERVER/>
  </SERVER_INFO>
</LOGIN>
</RIBCL>
```

Set host power example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
  <SERVER_INFO MODE="write">
    <!-- Modify the HOST_POWER attribute to toggle power on the host
server -->
    <!-- HOST_POWER="No" (Turns host server power off) -->
    <!-- A graceful shutdown will be attempted for ACPI-aware -->
    <!-- operating systems configured to support graceful shutdown. -->
    <!-- HOST_POWER="Yes" (Turns host server power on) -->
    <SET_HOST_POWER HOST_POWER="No"/>
  </SERVER_INFO>
</LOGIN>
</RIBCL>
```

GET_SERVER_NAME

The GET_SERVER_NAME command is used to retrieve the host server name used by the iLO 2. You can set this parameter using several methods, including the SERVER_NAME command, host RBSU, iLO 2 browser-based interface, and loading HP ProLiant Management Agents.

This command is supported by iLO 2 firmware version 1.30 or later. It is not supported by iLO or RILOE II.

Example:

```
<RIBCL version="2.21">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SERVER_INFO MODE="READ" >
      <GET_SERVER_NAME />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

iLO 2 maintains consistency between the various places the server name is used. The host RBSU has a two-line limitation of 14 characters each, or 28 characters of total server name text length.

Normally, HP ProLiant Management Agents are used to forward the server name attribute to iLO 2. This command can be used in instances where management agents are not used. However, the host operating system remains unaffected.

GET_SERVER_NAME return message

GET_SERVER_NAME returns the currently stored server name, if available. The server name is a quoted ASCII string and cannot be a network name. For example:

```
<SERVER_NAME VALUE="Linux Development Host" />
```

GET_SERVER_NAME runtime errors

None

SERVER_NAME

The SERVER_NAME command is used to assign the Server Name attribute shown in the user interface and host RBSU. This setting is not forwarded to the host operating system and does not affect the host operating system.

You must have the configure iLO 2 privilege to alter this attribute using the scripting interface. The SERVER_INFO section must be set to WRITE mode or an error is returned.

Example:

```
<RIBCL version="2.21">
  <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
    <SERVER_INFO MODE="write" >
      <SERVER_NAME VALUE = "Exchange05" />
    </SERVER_INFO>
  </LOGIN>
```

SERVER_NAME parameters

VALUE is a quoted ASCII string less than 50 characters in total length.

SERVER_NAME return message

There is no specific return message if this attribute is successfully set.

SERVER_NAME runtime errors

- If the configure iLO settings privilege is absent, a runtime error is returned.
- If SERVER_INFO is not opened for write, a runtime error is returned.

GET_EMBEDDED_HEALTH

GET_EMBEDDED_HEALTH command is used to retrieve health information of the server. For this command to parse correctly, the GET_EMBEDDED_HEALTH command must appear within a SERVER_INFO command block. You can set SERVER_INFO MODE to read or write.

Example:

```
<RIBCL VERSION="2.21">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="read">
      <GET_EMBEDDED_HEALTH />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

GET_EMBEDDED_HEALTH parameters

None

GET_EMBEDDED_HEALTH return messages

A possible GET_EMBEDDED_HEALTH_DATA return message is:

```
IP Address is: 16.100.000.192
cpqlocfg.exe: Receiving (116):
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
/>
</RIBCL>
cpqlocfg.exe: Receiving (116):
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
<RESPONSE
  STATUS="0x0000"
  MESSAGE='No error'
/>
<GET_EMBEDDED_HEALTH_DATA>
<FANS>
  <FAN>
    <LABEL VALUE = "Fan Block 1"/>
    <ZONE VALUE = "Power Supply"/>
```



```

        <STATUS VALUE = "Ok"/>
        <SPEED VALUE = "25" UNIT="Percentage"/>
    </FAN>
    <FAN>
        <LABEL VALUE = "Fan Block 2"/>
        <ZONE VALUE = "CPU 2"/>
        <STATUS VALUE = "Ok"/>
        <SPEED VALUE = "37" UNIT="Percentage"/>
    </FAN>
</FANS>
<TEMPERATURE>
    <TEMP>
        <LABEL VALUE = "Temp 1"/>
        <LOCATION VALUE = "I/O Board"/>
        <STATUS VALUE = "Ok"/>
        <CURRENTREADING VALUE = "29" UNIT="Celsius"/>
        <CAUTION VALUE = "65" UNIT="Celsius"/>
        <CRITICAL VALUE = "70" UNIT="Celsius"/>
    </TEMP>
    <TEMP>
        <LABEL VALUE = "Temp 2"/>
        <LOCATION VALUE = "Ambient"/>
        <STATUS VALUE = "Failed"/>
        <CURRENTREADING VALUE = "66" UNIT="Celsius"/>
        <CAUTION VALUE = "40" UNIT="Celsius"/>
        <CRITICAL VALUE = "45" UNIT="Celsius"/>
    </TEMP>
    <TEMP>
        <LABEL VALUE = "Temp 3"/>
        <LOCATION VALUE = "CPU 1"/>
        <STATUS VALUE = "Ok"/>
        <CURRENTREADING VALUE = "36" UNIT="Celsius"/>
        <CAUTION VALUE = "90" UNIT="Celsius"/>
        <CRITICAL VALUE = "95" UNIT="Celsius"/>
    </TEMP>
    <TEMP>
        <LABEL VALUE = "Temp 4"/>
        <LOCATION VALUE = "CPU 1"/>
        <STATUS VALUE = "Ok"/>
        <CURRENTREADING VALUE = "32" UNIT="Celsius"/>
        <CAUTION VALUE = "90" UNIT="Celsius"/>
        <CRITICAL VALUE = "95" UNIT="Celsius"/>
    </TEMP>
    <TEMP>

```

```

    <LABEL VALUE = "Temp 5"/>
    <LOCATION VALUE = "Power Supply"/>
    <STATUS VALUE = "Ok"/>
    <CURRENTREADING VALUE = "32" UNIT="Celsius"/>
    <CAUTION VALUE = "51" UNIT="Celsius"/>
    <CRITICAL VALUE = "56" UNIT="Celsius"/>
  </TEMP>
</TEMPERATURE>
<VRM>
</VRM>
<POWER_SUPPLIES>
</POWER_SUPPLIES>
<HEALTH_AT_A_GLANCE>
  <FANS STATUS= "Ok"/>
  <FANS REDUNDANCY= "Fully Redundant"/>
  <TEMPERATURE STATUS= "FAILED"/>
  <VRM STATUS= "Ok"/>
  <POWER_SUPPLIES STATUS= "Ok"/>
  <POWER_SUPPLIES REDUNDANCY= "unknown"/>
</HEALTH_AT_A_GLANCE>
</GET_EMBEDDED_HEALTH_DATA>
</RIBCL>
cpqlocfg.exe: Script succeeded on "16.100.000.192:000"

```

GET_POWER_READINGS

The GET_POWER_READINGS command is used to get the power readings from the server power supply.

GET_POWER_READINGS parameters

None

GET_POWER_READINGS return messages

Two types of responses are available from the GET_POWER_READINGS command, depending on whether or not an advanced license is applied.

If an advanced license is not applied, then a typical response is:

```

<?xml version="1.0"?>
<RIBCL VERSION="2.22">
  <RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
  />
  <GET_POWER_READINGS>
  <PRESENT_POWER_READING VALUE="275" UNIT="Watts"/>
  <!--
Additional information is available with iLO 2 Advanced and iLO 2 Select
licenses.
-->
</GET_POWER_READINGS>
</RIBCL>

```

```
cpqlocfg.exe: Script succeeded on "16.100.100.100:100"
```

If an advanced license is applied, a typical response is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
  <RESPONSE
    STATUS="0x0000"
    MESSAGE='No error'
  />
  <GET_POWER_READINGS>
    <PRESENT_POWER_READING VALUE="275" UNIT="Watts"/>
    <AVERAGE_POWER_READING VALUE="278" UNIT="Watts"/>
    <MAXIMUM_POWER_READING VALUE="283" UNIT="Watts"/>
    <MINIMUM_POWER_READING VALUE="270" UNIT="Watts"/>
  </GET_POWER_READINGS>
</RIBCL>
```

GET_POWER_CAP

The GET_POWER_CAP command is used to get the power cap of the server. For this command to parse correctly, the GET_POWER_CAP command must appear within a SERVER_INFO command block, and SERVER_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.21">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="read">
      <GET_POWER_CAP />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

GET_POWER_CAP parameters

None

GET_POWER_CAP return messages

A cap value of zero indicates that a power cap is not currently set on the server. A typical response is:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="read">
      <GET_POWER_CAP />
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

SET_POWER_CAP

The SET_POWER_CAP command is used to set a power cap on the server. For this command to parse correctly, the SET_POWER_CAP command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. You must have the configure iLO 2 privilege to execute this command.

You cannot set this property if a dynamic power cap is set for the server. Dynamic power capping is set and modified using either Onboard Administrator or Insight Power Manager.

Example of disabling the power cap:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <SET_POWER_CAP POWER_CAP="300"/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

SET_POWER_CAP parameters

SET_POWER_CAP POWER_CAP is the power cap on the server. Valid power cap values are determined using a power test run on the server at boot. The possible values are 0 to disable the power cap, or a numeric value in watts (as determined in the power test.)

SET_POWER_CAP runtime errors

The possible SET_POWER_CAP error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Power Regulator feature is not supported on this server.
- User does not have correct privilege for action.
- The power cap value is invalid.

GET_HOST_POWER_SAVER_STATUS

The GET_HOST_POWER_SAVER_STATUS command requests the state of the processor power regulator feature of the server. For this command to parse correctly, the GET_HOST_POWER_SAVER_STATUS command must appear within a SERVER_INFO command block. You can set SERVER_INFO MODE to read or write.

Example:

```
<RIBCL VERSION="2.0">
  <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
      <GET_HOST_POWER_SAVER_STATUS/>
    </SERVER_INFO>
  </LOGIN>
</RIBCL>
```

GET_HOST_POWER_SAVER_STATUS parameters

None

GET_HOST_POWER_SAVER_STATUS runtime errors

The possible GET_HOST_POWER_SAVER_STATUS error messages include:

- Feature not supported

GET_HOST_POWER_SAVER_STATUS return messages

The following information is returned within one of the following responses:

- ```
<GET_HOST_POWER_SAVER
 HOST_POWER_SAVER="OFF"
/>
```
- ```
<GET_HOST_POWER_SAVER
  HOST_POWER_SAVER="MIN"
/>
```
- ```
<GET_HOST_POWER_SAVER
 HOST_POWER_SAVER="AUTO"
/>
```

## SET\_HOST\_POWER\_SAVER

The SET\_HOST\_POWER\_SAVER command is used to set the Power Regulator Setting for the server processor. For this command to parse correctly, the SET\_HOST\_POWER\_SAVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <SET_HOST_POWER_SAVER HOST_POWER_SAVER="1"/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

## SET\_HOST\_POWER\_SAVER parameters

The HOST\_POWER\_SAVER command controls the Dynamic Power Saver feature of the server processor if the feature is supported. The possible values are:

- 1—Operating system control mode
- 2—HP Static Low Power mode
- 3—HP Dynamic Power Savings mode
- 4—HP Static High Performance mode

## SET\_HOST\_POWER\_SAVER runtime errors

The possible SET\_HOST\_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Power Regulator feature is not supported on this server.

- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.

## GET\_HOST\_POWER\_REG\_INFO

The GET\_HOST\_POWER\_REG\_INFO command requests iLO 2 power regulator information. For this command to parse correctly, the GET\_HOST\_POWER\_REG\_INFO command must appear within a SERVER\_INFO command block, and SERVER\_INFO\_MODE must be set to read.

Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="read">
 <GET_HOST_POWER_REG_INFO/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

## GET\_HOST\_POWER\_REG\_INFO parameters

None

## GET\_HOST\_POWER\_REG\_INFO runtime errors

GET\_HOST\_POWER\_REG\_INFO returns a runtime error if an iLO 2 Advanced License is not found. For example:

```
<RIBCL VERSION="2.22">
 <RESPONSE
 STATUS="0x0043"
 MESSAGE='This feature requires an advanced license'
 />
</RIBCL>
```

## GET\_HOST\_POWER\_REG\_INFO return messages

The GET\_HOST\_POWER\_REG\_INFO command returns all data available at the time of the request. If the request occurs within the first five minutes of a system or iLO 2 reset or power cycle, only a limited amount of data is available.

A possible GET\_HOST\_POWER\_REG\_INFO return message within the five minutes of a system or iLO 2 reset or power cycle is:

```
<GET_HOST_POWER_REG_INFO>
<NumberProcessors>0</NumberProcessors>
<NumberPstates>0</NumberPstates>
</GET_HOST_POWER_REG_INFO>
```

A possible GET\_HOST\_POWER\_REG\_INFO return message when all data is available is:

```
<GET_HOST_POWER_REG_INFO>
<NumberProcessors>2</NumberProcessors>
<NumberPstates>3</NumberPstates>
<Processor0>
<CurrentPstate>2</CurrentPstate>
<Pstate0>
<TotalAverage>34.3</TotalAverage>
```

```

</Pstate0>
<Pstate1>
<TotalAverage>0</TotalAverage>
</Pstate1>
<Pstate2>
<TotalAverage>65.7</TotalAverage>
</Pstate2>
<Pstate3>
<TotalAverage>0</TotalAverage>
</Pstate3>
.....
<Pstate7>
<TotalAverage>0</TotalAverage>
</Pstate7>
</Processor0>

<Processor1>
<CurrentPstate>2</CurrentPstate>
<Pstate0>
<TotalAverage>34.3</TotalAverage>
</Pstate0>
<Pstate1>
<TotalAverage>0</TotalAverage>
</Pstate1>
<Pstate2>
<TotalAverage>65.7</TotalAverage>
</Pstate2>
<Pstate3>
.....
<Pstate7>
<TotalAverage>0</TotalAverage>
</Pstate7>
</Processor1>
</GET_HOST_POWER_REG_INFO>

```

## GET\_HOST\_POWER\_STATUS

The GET\_HOST\_POWER\_STATUS command requests the power state of the server. For this command to parse correctly, the GET\_HOST\_POWER\_STATUS command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read or write.

Example:

```

<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <GET_HOST_POWER_STATUS/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>

```

## GET\_HOST\_POWER\_STATUS Parameters

None

## GET\_HOST\_POWER\_STATUS Runtime Errors

The possible GET\_HOST\_POWER\_STATUS error messages include:

- Host power is OFF.
- Host power is ON.

## GET\_HOST\_POWER\_STATUS Return Messages

The following information is returned within the response:

```
<GET_HOST_POWER
 HOST_POWER="OFF"
/>
```

## SET\_HOST\_POWER

The SET\_HOST\_POWER command is used to toggle the power button of server. For this command to parse correctly, the SET\_HOST\_POWER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <SET_HOST_POWER HOST_POWER="Yes"/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

## SET\_HOST\_POWER Parameters

HOST\_POWER enables or disables the Virtual Power Button. The possible values are "Yes" or "No."

## SET\_HOST\_POWER Runtime Errors

The possible SET\_HOST\_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Virtual Power Button feature is not supported on this server.
- Host power is already ON.
- Host power is already OFF.
- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.

## GET\_HOST\_PWR\_MICRO\_VER

The GET\_HOST\_PWR\_MICRO\_VER command toggles the power button of server. For this command to parse correctly, the GET\_HOST\_PWR\_MICRO\_VER command must appear within a SERVER\_INFO command block, and SERVER\_INFO must be set to read.



Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="admin" PASSWORD="admin123">
 <SERVER_INFO MODE="read">
 <GET_HOST_PWR_MICRO_VER/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

## GET\_HOST\_PWR\_MICRO\_VER parameters

None

## GET\_HOST\_PWR\_MICRO\_VER runtime errors

The possible GET\_HOST\_PWR\_MICRO\_VER error messages include:

- Error if the power micro cannot be read (hardware problem).
- Power Off if the server is powered off.
- N/A if the server does not support a power micro.

## GET\_HOST\_PWR\_MICRO\_VER return messages

- No errors and displays version information:  
<GET\_HOST\_PWR\_MICRO\_VER>  
 <PWR\_MICRO VERSION="2.3"/>  
</GET\_HOST\_PWR\_MICRO\_VER>
- Server powered off:  
<GET\_HOST\_PWR\_MICRO\_VER>  
 <PWR\_MICRO VERSION="OFF"/>  
</GET\_HOST\_PWR\_MICRO\_VER>
- Power micro not supported on the server:  
<GET\_HOST\_PWR\_MICRO\_VER>  
 <PWR\_MICRO VERSION="N/A"/>  
</GET\_HOST\_PWR\_MICRO\_VER>
- Failed to read power micro version:  
<GET\_HOST\_PWR\_MICRO\_VER>  
 <PWR\_MICRO VERSION="Error"/>  
</GET\_HOST\_PWR\_MICRO\_VER>

## GET\_PWREG\_CAPABILITIES

The GET\_PWREG\_CAPABILITIES command requests iLO 2 power regulator information related to system power minimum and maximum values, power supply type and capacity, and power microprocessor firmware version. For this command to parse correctly, the GET\_PWREG\_CAPABILITIES command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to read.

Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
```

```

 <SERVER_INFO MODE="read">
 <GET_PWREG_CAPABILITIES/>
 </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## GET\_PWREG\_CAPABILITIES parameters

None

## GET\_PWREG\_CAPABILITIES runtime errors

The possible GET\_PWREG\_CAPABILITIES error messages include:

- Error if the power micro cannot be read (hardware problem).
- Power Off if the server is powered off.
- N/A if the server does not support a power micro.

## GET\_PWREG\_CAPABILITIES return messages

```

<GET_PWREG_CAPABILITIES>
 <FWVERSION>"1.77"</FWVERSION>
 <THRD ID="0" SOCKET="1" CORE="0" THREAD="0"/>
 <QS Q="0" P="0" L="100"/>
 <QS Q="1" P="1" L="75"/>
 <QS Q="2" P="1" L="75"/>
 <QS Q="3" P="1" L="75"/>
 <QS Q="4" P="1" L="75"/>
 <QS Q="5" P="1" L="75"/>
 <QS Q="6" P="1" L="75"/>
 <QS Q="7" P="1" L="75"/>
 <QS Q="8" P="1" L="75"/>
 <THRD ID="1" SOCKET="1" CORE="1" THREAD="0"/>
 <QS Q="0" P="0" L="100"/>
 <QS Q="1" P="1" L="75"/>
 <QS Q="2" P="1" L="75"/>
 <QS Q="3" P="1" L="75"/>
 <QS Q="4" P="1" L="75"/>
 <QS Q="5" P="1" L="75"/>
 <QS Q="6" P="1" L="75"/>
 <QS Q="7" P="1" L="75"/>
 <QS Q="8" P="1" L="75"/>
 <THRD ID="2" SOCKET="1" CORE="2" THREAD="0"/>
 <QS Q="0" P="0" L="100"/>
 <QS Q="1" P="1" L="75"/>
 <QS Q="2" P="1" L="75"/>
 <QS Q="3" P="1" L="75"/>

```

```

<QS Q="4" P="1" L="75"/>
<QS Q="5" P="1" L="75"/>
<QS Q="6" P="1" L="75"/>
<QS Q="7" P="1" L="75"/>
<QS Q="8" P="1" L="75"/>
<THRD ID="3" SOCKET="1" CORE="3" THREAD="0"/>
<QS Q="0" P="0" L="100"/>
<QS Q="1" P="1" L="75"/>
<QS Q="2" P="1" L="75"/>
<QS Q="3" P="1" L="75"/>
<QS Q="4" P="1" L="75"/>
<QS Q="5" P="1" L="75"/>
<QS Q="6" P="1" L="75"/>
<QS Q="7" P="1" L="75"/>
<QS Q="8" P="1" L="75"/>
<EFFICIENCY_MODE INDEX="0" NAME="OSC">"OS_Control"</EFFICIENCY_MODE>
<EFFICIENCY_MODE INDEX="1" NAME="MIN">"Low_Power"</EFFICIENCY_MODE>
<EFFICIENCY_MODE INDEX="2" NAME="DYN">"Dynamic"</EFFICIENCY_MODE>
<EFFICIENCY_MODE INDEX="3" NAME="MAX">"Max_Power"</EFFICIENCY_MODE>
<HISTORY SIZE="288" INTERVAL="300" TRACE="10"/>
<BUSYMAXPWR>203</BUSYMAXPWR>
<IDLEMAXPWR>168</IDLEMAXPWR>
<ECAP/>
<TEMP/>
<CPU/>
<PWRSPPLY TYPE="AC" CAPACITY="800"/>
<PWRALERT VERSION="0"/>
<PWR MICRO VERSION="3.3"/>
</GET_PWREG_CAPABILITIES>

```

## RESET\_SERVER

The RESET\_SERVER command will force a warm boot of the server, if the server is currently on. For this command to parse correctly, the RESET\_SERVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```

<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <RESET_SERVER/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>

```

## RESET\_SERVER errors

The possible RESET\_SERVER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Server is currently powered off.
- User does NOT have correct privilege for action. RESET\_SERVER\_PRIV required.

## RESET\_SERVER parameters

None

## PRESS\_PWR\_BTN

This PRESS\_PWR\_BTN command is used to simulate a physical press of the server power button. For this command to parse correctly, the PRESS\_PWR\_BTN command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <PRESS_PWR_BTN/>
 </SERVER_INFO>
</LOGIN>
</RIBCL>
```

## PRESS\_PWR\_BTN parameters

There are no parameters for this command.

## PRESS\_PWR\_BTN runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.

## HOLD\_PWR\_BTN

This HOLD\_PWR\_BTN command is used to simulate a physical press and hold of the server power button. For this command to parse correctly, the HOLD\_PWR\_BTN command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <HOLD_PWR_BTN/>
 </SERVER_INFO>
</LOGIN>
</RIBCL>
```

```
</SERVER_INFO>
</LOGIN>
</RIBCL>
```

## HOLD\_PWR\_BTN parameters

There are no parameters for this command.

## HOLD\_PWR\_BTN runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.

## COLD\_BOOT\_SERVER

This COLD\_BOOT\_SERVER command will force a cold boot of the server, if the server is currently on. For this command to parse correctly, the COLD\_BOOT\_SERVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <COLD_BOOT_SERVER/>
 </SERVER_INFO>
</LOGIN>
</RIBCL>
```

## COLD\_BOOT\_SERVER parameters

There are no parameters for this command.

## COLD\_BOOT\_SERVER runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Host power is already OFF.
- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.

## WARM\_BOOT\_SERVER

This WARM\_BOOT\_SERVER command will force a warm boot of the server, if the server is currently on. For this command to parse correctly, the WARM\_BOOT\_SERVER command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
```

```

<LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <WARM_BOOT_SERVER/>
 </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## WARM\_BOOT\_SERVER parameters

There are no parameters for this command.

## WARM\_BOOT\_SERVER runtime errors

The possible error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Host power is already OFF.
- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.

## SERVER\_AUTO\_PWR

The SERVER\_AUTO\_PWR command is used to set the automatic power on and power on delay settings of the server.

This command is supported by iLO 2 firmware version 1.20 or later. It is not supported by iLO firmware or RILOE II.

Example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <!-- Enable automatic power on with 30 seconds delay -->
 <SERVER_AUTO_PWR VALUE="30" />
 </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## SERVER\_AUTO\_PWR parameters

The possible values are:

- Yes enables automatic power on with a minimum delay.
- No disables automatic power on.
- 15 enables automatic power on with 15-second delay.
- 30 enables automatic power on with 30-second delay.
- 45 enables automatic power on with 45-second delay.
- 60 enables automatic power on with 60-second delay.
- Random enables automatic power on with random delay up to 60-second.

## SERVER\_AUTO\_PWR runtime errors

The possible error messages include:

- User does not have correct privilege for action. RESET\_SERVER\_PRIV required.
- The value specified for SERVER\_AUTO\_PWR is invalid.

## GET\_SERVER\_AUTO\_PWR

The GET\_SERVER\_AUTO\_PWR command is used to get the automatic power on and power on delay settings of the server.

Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SERVER_INFO MODE="read">
 <GET_SERVER_AUTO_PWR />
 </SERVER_INFO>
 </LOGIN>
</RIBCL>
```

## GET\_SERVER\_AUTO\_PWR parameters

None

## GET\_SERVER\_AUTO\_PWR return message

A possible GET\_SERVER\_AUTO\_PWR return is:

```
<?xml version="1.0"?>
<RIBCL VERSION="2.22">
 <RESPONSE
 STATUS="0x0000"
 MESSAGE='No error'
 />
 <GET_SERVER_AUTO_PWR>
 <!--
 Automatically Power On Server is enabled
 with 30 seconds power on delay.
 -->
 <SERVER_AUTO_PWR VALUE="30" />
 </GET_SERVER_AUTO_PWR>
</RIBCL>
```

## GET\_UID\_STATUS

The GET\_UID\_STATUS command requests the state of the server UID. For this command to parse correctly, the GET\_UID\_STATUS command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read or write.

Example:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
```

```

 <SERVER_INFO MODE="write">
 <GET_UID_STATUS />
 </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## GET\_UID\_STATUS parameters

None

## GET\_UID\_STATUS response

The following information is returned within the response:

```

<GET_UID_STATUS
 UID="OFF"
/>

```

## UID\_CONTROL

The UID\_CONTROL command toggles the server UID. For this command to parse correctly, the UID\_CONTROL command must appear within a SERVER\_INFO command block, and SERVER\_INFO MODE must be set to write.

Example:

```

<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <SERVER_INFO MODE="write">
 <UID_CONTROL UID="Yes"/>
 </SERVER_INFO>
 </LOGIN>
</RIBCL>

```

## UID\_CONTROL parameters

UID determines the state of the UID. A value of "Yes" turns the UID light on, and a value of "No" turns the UID light off.

## UID\_CONTROL errors

The possible UID\_CONTROL error messages include:

- UID is already ON.
- UID is already OFF.

## GET\_VPB\_CABLE\_STATUS (RILOE II only)

The GET\_VPB\_CABLE\_STATUS to return the status of the Virtual Power Button cable that may be connected to a RILOE II board. For this command to parse correctly, the GET\_VPB\_CABLE\_STATUS command must appear within a SERVER\_INFO command block. You can set SERVER\_INFO MODE to read or write.

```

<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">

```



```

 <SERVER_INFO MODE="read">
 <GET_VPB_CABLE_STATUS/>
 </SERVER_INFO>
</LOGIN>
</RIBCL>

```

## GET\_VPB\_CABLE\_STATUS parameters

None

## GET\_VPB\_CABLE\_STATUS Runtime Errors

The possible GET\_VPB\_CABLE\_STATUS error messages include:

- Virtual Power Button cable is attached.
- Virtual Power Button cable is not attached.

## GET\_VPB\_CABLE\_STATUS return messages

A possible GET\_VPB\_CABLE\_STATUS return message is:

```

<RIBCL VERSION="2.22">
 <RESPONSE
 STATUS="0x0000"
 MESSAGE='No error'
 />
 <GET_VPB_CABLE>
 <VIRTUAL POWER BUTTON CABLE="ATTACHED"/>
 </GET_VPB_CABLE>
</RIBCL>

```

# SSO\_INFO

The SSO\_INFO MODE command can only appear within a LOGIN command block. Only commands that are SSO\_INFO MODE-type commands are valid inside the SSO\_INFO MODE command block.

SSO\_INFO MODE requires the MODE parameter with a value of read or write. MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information.

Write mode enables both reading and writing of iLO 2 information. Read mode prevents modification of the iLO 2 information. You must have the Configure iLO 2 privilege to execute this command.

Example:

```

<SSO_INFO MODE="write">
..... SSO_INFOcommands
</SSO_INFO>

```

Deleting a SSO HP SIM Server Record by index number example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SSO_INFO MODE="write">
 <DELETE_SERVER INDEX="6" />

```

```

 </SSO_INFO>
</LOGIN>
</RIBCL>

```

SSO\_INFO is only supported on licensed, iLO 2 v1.30 firmware. If iLO 2 is not licensed, you can still modify these settings. iLO 2 does not return an error. However, any SSO attempt is rejected if a license is not present. See the *HP Integrated Lights-Out 2 User Guide* for more information.

## GET\_SSO\_SETTINGS

GET\_SSO\_SETTINGS command is used to retrieve SSO settings for iLO 2. For this command to parse correctly, the GET\_SSO\_SETTINGS command must appear within a SSO\_INFO command block, and SSO\_INFO MODE can be set to read or write.

Example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SSO_INFO MODE="read">
 <GET_SSO_SETTINGS/>
 </SSO_INFO>
</LOGIN>
</RIBCL>

```

## GET\_SSO\_SETTINGS parameters

None

## GET\_SSO\_SETTINGS return messages

The following is an example of an SSO settings response from a configured iLO 2. There are 0 or more SSO\_SERVER records reflecting the number of stored server records in each.

```

<GET_SSO_SETTINGS>
<TRUST_MODE VALUE="CERTIFICATE" />
<USER_ROLE LOGIN_PRIV="Y" />
<USER_ROLE REMOTE_CONS_PRIV="N" />
<USER_ROLE RESET_SERVER_PRIV="N" />
<USER_ROLE VIRTUAL_MEDIA_PRIV="N" />
<USER_ROLE CONFIG_ILO_PRIV="N" />
<USER_ROLE ADMIN_PRIV="N" />
<OPERATOR_ROLE LOGIN_PRIV="Y" />
<OPERATOR_ROLE REMOTE_CONS_PRIV="Y" />
<OPERATOR_ROLE RESET_SERVER_PRIV="Y" />
<OPERATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<OPERATOR_ROLE CONFIG_ILO_PRIV="N" />
<OPERATOR_ROLE ADMIN_PRIV="N" />
<ADMINISTRATOR_ROLE LOGIN_PRIV="Y" />
<ADMINISTRATOR_ROLE REMOTE_CONS_PRIV="Y" />
<ADMINISTRATOR_ROLE RESET_SERVER_PRIV="Y" />
<ADMINISTRATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
<ADMINISTRATOR_ROLE CONFIG_ILO_PRIV="Y" />
<ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />
<SSO_SERVER INDEX="0"
 ISSUED_TO="viv.hp.com"
 ISSUED_BY="viv.hp.com"
 VALID_FROM="061108192059Z"

```

```

 VALID_UNTIL="161108192059Z">
-----BEGIN CERTIFICATE-----
.
.
.
-----END CERTIFICATE-----
</SSO_SERVER>
<SSO_SERVER INDEX="1">
ant.hp.com
</SSO_SERVER>
</GET_SSO_SETTINGS>

```

## MOD\_SSO\_SETTINGS

The MOD\_SSO\_SETTINGS command is used to modify the HP SSO settings for iLO 2. For this command to parse correctly, the MOD\_SSO\_SETTINGS command must appear within a SSO\_INFO command block, and SSO\_INFO MODE must be set to write. The user must have the Configure iLO 2 privilege to execute this command.

Example:

```

<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SSO_INFO MODE="write">
 <MOD_SSO_SETTINGS>
 <!-- Specify the desired trust mode Options: DISABLED(default),
 CERTIFICATE (recommended), NAME, or ALL
 -->

 <TRUST_MODE="CERTIFICATE" />

 <!-- Specify the privileges assigned to the user role -->
 <USER_ROLE LOGIN_PRIV="Y" />
 <USER_ROLE REMOTE_CONS_PRIV="N" />
 <USER_ROLE RESET_SERVER_PRIV="N" />
 <USER_ROLE VIRTUAL_MEDIA_PRIV="N" />
 <USER_ROLE CONFIG_ILO_PRIV="N" />
 <USER_ROLE ADMIN_PRIV="N" />

 <!-- Specify the privileges assigned to the operator role -->
 <OPERATOR_ROLE LOGIN_PRIV="Y" />
 <OPERATOR_ROLE REMOTE_CONS_PRIV="Y" />
 <OPERATOR_ROLE RESET_SERVER_PRIV="Y" />
 <OPERATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
 <OPERATOR_ROLE CONFIG_ILO_PRIV="N" />
 <OPERATOR_ROLE ADMIN_PRIV="N" />

 <!-- Specify the privileges assigned to the administrator role -->
 <ADMINISTRATOR_ROLE LOGIN_PRIV="Y" />

```

```

 <ADMINISTRATOR_ROLE REMOTE_CONS_PRIV="Y" />
 <ADMINISTRATOR_ROLE RESET_SERVER_PRIV="Y" />
 <ADMINISTRATOR_ROLE VIRTUAL_MEDIA_PRIV="Y" />
 <ADMINISTRATOR_ROLE CONFIG_ILO_PRIV="Y" />
 <ADMINISTRATOR_ROLE ADMIN_PRIV="Y" />

 </MOD_SSO_SETTINGS>
</SSO_INFO>
</LOGIN>
</RIBCL>

```

## MOD\_SSO\_SETTINGS parameters

TRUST\_MODE sets the Single Sign-On trust mode. The current setting is unaltered if this setting is omitted from the script. Accepted values:

- Disabled—Disables HP SIM SSO on this processor.
- Certificate—Accepts only SSO requests authenticated using a certificate.
- Name—Trusts SSO requests from the named HP SIM Server.
- All—Accepts any SSO request from the network.

Role names are used to associate iLO privileges. The specified privileges are set accordingly for that role, and a privilege that is omitted is unaltered. Enable a privilege for the role using the argument "Y" and disable the privilege for the role using the argument "N."

There are three roles for privilege assignment. Omitting a role leaves the current assignment unaltered:

- USER\_ROLE—Privileges associated with User
- OPERATOR\_ROLE—Privileges associated with Operator
- ADMINISTRATOR\_ROLE—Privileges associated with Administrator

For each role, there are multiple privileges that can be manipulated. The privilege is specified within the role tag. If a privilege is omitted, the current value is unaltered. Each privilege assignment is Boolean and can be set to "Y" (privilege granted) or "N" (privilege denied). For more details on account privileges, see the User Administration section of the User Guide.

- LOGIN\_PRIV—Allows login for this role.
- REMOTE\_CONS\_PRIV—Grants access to remote console resources.
- RESET\_SERVER\_PRIV—Grants access to power and reset controls.
- VIRTUAL\_MEDIA\_PRIV—Grants access to virtual media resources.
- CONFIG\_ILO\_PRIV—Allows settings modification.
- ADMIN\_PRIV—Allows local user account modification.

## MOD\_SSO\_SETTINGS runtime errors

- Incorrect firmware version. SSO is only supported on iLO 2 v1.30 firmware or later.
- User does not have correct privilege for action. CONFIG\_ILO\_PRIV required.
- SSO\_INFO must be in write mode.

## SSO\_SERVER

SSO\_SERVER command is used to create HP SIM Trusted SSO Server records. For this command to parse correctly, it must appear within a SSO\_INFO command block, and SSO\_INFO MODE must be set to write. You must have the Configure iLO 2 privilege to execute this command. This command can be combined with MOD\_SSO\_SETTINGS.

You can specify multiple SSO server records by using multiple instances of this command. The servers are added in the order that the records are specified. Duplicate records may be rejected and generate an error. The number of records stored by the lights-out processor depends on the size of the entries because certificates do not have a fixed size. Multiple certificates can normally be stored.

There are three ways to add an HP SIM Trusted Server record using this command:

- The server can be specified by network name (requires SSO trust level set to trust by name or trust all, but is not supported for trust by certificate). Use the fully qualified network name.
- The server certificate can be imported by iLO 2 (the LOM processor requests the certificate from the specified HP SIM server using anonymous HTTP request). The iLO 2 processor must be able to contact the HP SIM server on the network at the time this command is processed for this method to work.
- The server certificate can be directly installed on iLO 2. However, you must obtain the x.509 certificate in advance. This method enables you to configure the iLO 2 in advance of placing it on the network with the HP SIM server. It also allows you to verify the contents of the HP SIM server certificate. See the *HP Integrated Lights-Out 2 User Guide* or the HP SIM User Guide for additional methods of obtaining the certificate from the HP SIM server.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
<SSO_INFO MODE="write">
<!-- Add an SSO server record using the network name
(works for TRUST_MODE NAME or ALL) -->
<SSO_SERVER NAME="hpsim1.hp.net" />

<!-- Add an SSO server record using indirect iLO import
from the network name -->
<SSO_SERVER IMPORT_FROM="hpsim2.hp.net" />

<!-- Add an SSO server certificate record using direct
import of certificate data -->
<IMPORT_CERTIFICATE>
-----BEGIN CERTIFICATE-----
.
.
.
-----END CERTIFICATE-----
</IMPORT_CERTIFICATE>
</SSO_INFO>
</LOGIN>
</RIBCL>
```

## SSO\_SERVER parameters

NAME indicates that the server is being specified by network name. It receives a quoted string containing the fully qualified network name of the HP SIM Trusted Server. The name is not validated by iLO 2 until an SSO login is attempted. For example, the syntax to add an HP SIM Trusted Server name:

```
<SSO_SERVER NAME="hpsim1.hp.net" />
```

IMPORT\_FROM indicates that iLO 2 should request the HP SIM Trusted Server certificate from HP SIM.

This request is implemented using an anonymous HTTP request similar to:

```
http://<sim network address>:280/GetCertificate
```

iLO 2 requests the certificate when this command is processed. If the HP SIM server is unreachable, then an error occurs. For example, the syntax to have iLO 2 import a server certificate resembles:

```
<SSO_SERVER IMPORT_FROM="hpsim2.hp.net" />
```

IMPORT\_CERTIFICATE indicates that iLO 2 should import the literal .PEM encoded x.509 certificate data that follows. The data is encoded in a block of text that includes the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- text. For example, the syntax to import an HP SIM Trusted Server certificate resembles the following:

```
<SSO_SERVER>
-----BEGIN CERTIFICATE-----
MIIC3TCCAkYCBESzwFUwDQYJKoZIhvcNAQEFBQAwgbUxCzAJBgNVBAYTA1VTMRMwE.....
.....
kXzhuVzPfWzQ+a2E9tGAE/YgNGTfS9vKkVLUf6QoP/RQpYpk15BxrsN3gM/PeT3zrxyTleE=
-----END CERTIFICATE-----
</SSO_SERVER>
```

The certificate is validated by iLO 2 to assure that it can be decoded before it is stored. An error results if the certificate is a duplicate or corrupt.

iLO 2 does not support certificate revocation and does not honor certificates that appear expired. You must remove any revoked or expired certificates.

## SSO\_SERVER runtime errors

A runtime error is generated:

- If a certificate is a duplicate.
- If a certificate is corrupt.
- If the HP SIM server cannot be contacted using IMPORT\_FROM.
- If the HP SIM Trusted Server database is full. You must delete other records to make sufficient room to add a new entry.
- If the trust mode is set incorrectly.

## DELETE\_SERVER

The DELETE\_SERVER command is used to remove an HP SIM Trusted SSO Server record. For this command to parse correctly, it must appear within a SSO\_INFO command block, and SSO\_INFO MODE must be set to write. You must have the Configure iLO 2 privilege to execute this command.

You can specify multiple SSO server records by using multiple instances of this command. The servers are deleted in the order that the records are specified, and the records are renumbered by each deletion. Delete records in the highest-to-lowest order if you want to delete multiple records at the same time.

Example:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="Administrator" PASSWORD="password">
 <SSO_INFO MODE="write">
 <DELETE_SERVER INDEX="6" />
 </SSO_INFO>
</LOGIN>
</RIBCL>
```

## DELETE\_SERVER parameters

INDEX indicates the record number to delete. This number is consistent with the index returned using a GET\_SSO\_SETTINGS command. The index is 0-based; that is the first record is index 0, the second record is index 1, and so on.

## DELETE\_SERVER runtime errors

A runtime error is generated if the index is invalid.

---

# HPQLOMGC command language

## Using HPQLOMGC

HPQLOMGC reads directory settings for the management processor from an XML file. The script used is a subset of the RIBCL and has been extended to support multiple management processor firmware images. HPQLOMGC does not operate on iLO 2 devices.

The following is an example of an XML file:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="user" PASSWORD="password">
 <DIR_INFO MODE="write">
 <ILO_CONFIG>
 <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\ilo140.brk" />
 </ILO_CONFIG>
 <RILOE_CONFIG>
 <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloe.brk" />
 </RILOE_CONFIG>
 <RILOE2_CONFIG>
 <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloeii.brk" />
 </RILOE2_CONFIG>
 <MOD_DIR_CONFIG>
 <DIR_AUTHENTICATION_ENABLED value="YES" />
 <DIR_LOCAL_USER_ACCT value="YES" />
 <DIR_SERVER_ADDRESS value="administration.wins.hp.com" />
 <DIR_SERVER_PORT value="636" />
 <DIR_OBJECT_DN value="CN=RILOP5,CN=Users,DC=RILOEGRP2,DC=HP" />
 <DIR_OBJECT_PASSWORD value="aurora" />
 <DIR_USER_CONTEXT_1 value="CN=Users,DC=RILOEGRP2,DC=HP" />
 <DIR_USER_CONTEXT_2 value="" />
 <DIR_USER_CONTEXT_3 value="" />
 <DIR_ROLE value="CN=RILOEROLE,CN=Users,DC=RILOEGRP2,DC=HP" />
 <DIR_LOGIN_NAME value="RILOEGRP2\Admin1" />
 <DIR_LOGIN_PASSWORD value="aurora" />
 </MOD_DIR_CONFIG>
</DIR_INFO>
</LOGIN>
</RIBCL>
```

## ILO\_CONFIG

RIBCL allows for only one firmware image per XML file. The command language for HPQLOMGC has been modified to allow for each management processor to have a specified firmware image within a single XML file. These commands must be displayed within a DIR\_INFO block, and DIR\_INFO must be in



write mode. The management processor is reset after the firmware upgrade is complete. To update the firmware, the user must be logged in with the appropriate privilege.

This command line uses the following parameters:

- UPDATE\_RIB\_FIRMWARE IMAGE\_LOCATION ("[UPDATE\\_RIB\\_FIRMWARE parameters](#)" on page [101](#))
- MOD\_DIR\_CONFIG

---

## iLO 2 ports

### Enabling the iLO 2 Shared Network Port feature through XML scripting

For information on how to use the SHARED\_NETWORK\_PORT command to enable the iLO 2 Shared Network Port through XML scripting, see the “Remote Insight command language (“Using RIBCL” on page 70)” section.

The following sample script configures the iLO 2 to select the Shared Network Port. You can customize this script to your needs. Using this script on platforms that do not support the Shared Network Port will cause an error.

```
<RIBCL version="2.21">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <RIB_INFO MODE="WRITE">
 <MOD_NETWORK_SETTINGS>
 <SHARED_NETWORK_PORT VALUE="Y" />
 </MOD_NETWORK_SETTINGS>
 </RIB_INFO>
 </LOGIN>
</RIBCL>
```

### Re-enabling the dedicated NIC management port

You can re-enable the iLO 2 dedicated NIC management port using the User Interface, RBSU, CLP, or XML. You can re-enable the iLO dedicated NIC management port using the iLO 2 RBSU or XML scripting. For information about how to use the SHARED\_NETWORK\_PORT command, see the section, “Using RIBCL (on page 70).”

To re-enable the dedicated management port using RBSU:

1. Connect the dedicated NIC management port to a LAN from which the server is managed.
2. Reboot the server.
3. When prompted during POST, press the **F8** key to enter iLO RBSU.
4. Select **Network>NIC>TCP/IP**, and press the **Enter** key.
5. In the Network Configuration menu, press **Space Bar** to change the Network Interface Adapter Field to ON.
6. Press the **F10** key to save the configuration.
7. Select **File>Exit**, and press the **Enter** key.

After the iLO resets, the dedicated management NIC port is active.

To re-enable the dedicated iLO using XML, use the following sample RIBCL script. The sample script configures the iLO to select the iLO Network Port. You can modify the script for your specific needs. Using this script on platforms that do not support the Shared Network Port causes an error.

```
<RIBCL version="2.21">
 <LOGIN USER_LOGIN="adminname" PASSWORD="password">
 <RIB_INFO MODE="WRITE">
 <MOD_NETWORK_SETTINGS>
 <SHARED_NETWORK_PORT VALUE="N" />
 </MOD_NETWORK_SETTINGS>
 </RIB_INFO>
 </LOGIN>
</RIBCL>
```

---

# iLO 2 parameters

## Status Summary parameters

Parameter	Definition
Server name	Displays the server name. If the Insight Management Agents are being used with the host server operating system, they will provide the iLO 2 with the server name.
UUID	Identifies the host. Although the UUID is assigned when the system is manufactured, you can change this setting using the system RBSU during POST.
Server Serial Number / Product ID	Identifies the serial number of the server. Although the Serial Number is assigned when the system is manufactured, you can change this setting using the system RBSU during POST.  The Product ID is used to distinguish between different systems with similar serial numbers. Although the Product ID is assigned when the system is manufactured, you can change this setting using the system RBSU during POST.
Virtual UUID	Appears when it is assigned by other software from HP. This value does not appear when it is not set.
Virtual Serial Number	The Virtual Serial Number is displayed when it is assigned by other software from HP. This value is not displayed when it is not set.
System Health	Represents the server internal health indicator, if supported. It summarizes problems with fans, temperature sensors, VRMs, and other monitored subsystems in the server. See the System Health page for details.
System ROM	The family and version of the active system ROM. If the system supports a backup system ROM, the backup date is also shown.
Internal Health LED	Represents the state of the Internal Health LED of the server when this page was loaded.
TPM Status	Represents the configuration status of Trusted Platform Module in the system.
Server Power	Displays if the host is powered ON, or in STANDBY (OFF) mode.

Parameter	Definition
UID Light	<p>Represents the state of the Unit Identification light when this page was loaded. You control the UID state using the button beside the UID icon in addition to the physical UID buttons on the server chassis.</p> <p>The UID helps you identify and locate a system and is used to indicate that a critical operation is in progress on the host, such as Remote console access or firmware update.</p> <p>The current state, ON or OFF, is the last state chosen using one of these methods. If a new state is chosen while the UID is blinking, this new state becomes the current state, and takes effect when the UID stops blinking. While the UID is blinking, the "current state" of the UID will be shown along with the tag (FLASHING). When the UID stops blinking, this tag is removed.</p>
Last Used Remote Console	Displays the previously launched remote console and availability. This allows you to quickly launch your preferred remote console. You may use the remote console if it is available and you have user privileges. If the console is in use, launching the remote console provides access to the acquire button. You can choose a different console by following the Last Used Remote Console link.
Latest IML Entry	The most recent entry in the Integrated Management Log.
iLO 2 Name	Displays the name assigned to the Integrated Lights-Out 2 subsystem. By default, this is iLO prepended to the system serial number. This value is used for the network name, so should be unique.
License Type	Displays whether the system has a feature license installed. Some features of iLO 2 cannot be accessed unless optionally licensed.
iLO 2 Firmware Version	Displays information about the version of iLO 2 firmware currently installed.
Active Sessions	Displays the users currently logged into iLO 2.
Latest iLO 2 Event Log Entry	Displays the most recent entry in the iLO 2 event log.
iLO 2 Date/Time	<p>Displays the date (MM/DD/YYYY) as indicated by the Integrated Lights-Out 2 subsystem internal clock.</p> <p>The iLO 2 internal clock is synchronized with the host system at POST and when the Insight Agents run.</p>

## User Administration parameters

Parameter	Default value	Definition
User name	Administrator	This parameter is the user's real name as it is displayed in the user list and event log. It is not the name used to log in. The maximum length of the user name is 39 characters.
Login name	Administrator	This is a case-sensitive name that the user must provide to log in to iLO 2.

Parameter	Default value	Definition
Password	A random, eight-character alphanumeric string that is factory assigned	This is a case-sensitive password that the user must provide to log in to iLO 2. In Security Options, the minimum password length can be assigned. The minimum password can be from 0 to 39 characters. The default minimum password length is eight characters. You must enter the password twice for verification.
Administer user accounts	Yes	This privilege allows a user to add, modify, and delete user accounts. It also allows the user to alter privileges for all users, including granting all permissions to a user.
Remote console access	Yes	This privilege allows a user to remotely manage the Remote Console of a managed system, including video, keyboard, and mouse controls.
Virtual power and reset	Yes	This privilege allows a user to power-cycle or reset the host platform.
Virtual media	Yes	This privilege allows a user to use virtual media on the host platform.
Configure iLO 2 settings	Yes	This privilege enables a user to configure most iLO 2 settings, including security settings. It does not include user account administration.  After iLO 2 is correctly configured, revoking this privilege from all users prevents reconfiguration. A user with the Administer User Accounts privilege can enable or disable this privilege. iLO 2 can also be reconfigured if iLO 2 RBSU is enabled.

## Global Settings parameters

Settings (parameters) found on the Access Options page of the iLO 2 user interface.

Parameter	Default value	Descriptions
Idle Connection Timeout (minutes)	30 minutes	This setting specifies the interval of user inactivity, in minutes, before the web server and Remote Console session automatically terminate. The following settings are valid: 15, 30, 60, 120 minutes, or 0 (infinite). The infinite timeout value does not log out inactive users.

Parameter	Default value	Descriptions
Lights-Out Functionality	Enabled	<p>This setting enables connection to iLO 2. If disabled, all connections to iLO 2 are prevented.</p> <p>The iLO 2 10/100 network and communications with operating system drivers are turned off if Lights-Out functionality is disabled. The iLO 2 Diagnostic Port for an HP ProLiant BL p Class server is also disabled.</p> <p>If iLO 2 functionality is disabled (including the iLO 2 Diagnostic Port), you must use the server's Security Override Switch to enable iLO 2. See your server documentation to locate the Security Override Switch and set it to override. Power up the server and use the iLO 2 RBSU to set Lights-Out Functionality to Enabled.</p>
iLO 2 ROM-Based Setup Utility	Enabled	<p>This setting enables or disables the iLO 2 ROM-Based Setup Utility. Normally, the iLO2 Option ROM prompts you to press <b>F8</b> to enter RBSU, but if iLO 2 is disabled or iLO 2 RBSU is disabled, the RBSU prompt is bypassed.</p>
Require Login for iLO 2 RBSU	Disabled	<p>This setting enables RBSU access with or without a user-credentials challenge. If this setting is Enabled, and you press <b>F8</b> during POST to enter iLO 2 RBSU, a login dialog box appears.</p>
Show iLO 2 during POST	Disabled	<p>This setting enables the display of the iLO 2 network IP address during the host server POST process.</p>
Serial Command Line Interface Status	Enabled-Authentication Required	<p>This setting enables you to change the login model of the CLI feature through the serial port. The following settings are valid:</p> <ul style="list-style-type: none"> <li>• Enabled—Authentication Required</li> <li>• Enabled—No Authentication</li> <li>• Disabled</li> </ul>
Serial Command Line Interface Speed	9600	<p>This setting enables you to use the serial port to change the speed of the serial port for the CLI feature. The following speeds (in bits/s) are valid: 9600, 19200, 38400, 57600, and 115200. The serial port configuration must be set to No parity, 8 data bits, and 1 stop bit (N/8/1) for proper operation. The serial port speed that is set by this parameter must match the speed of the serial port set in the System ROM RBSU setup.</p>
Minimum Password Length	8	<p>This setting specifies the minimum number of characters allowed when a user password is set or changed. The character length can be set at a value from 0 to 39.</p>
Server Name	—	<p>This setting enables you to specify the host server name. This value is assigned when using HP ProLiant Management Agents. If you do not use the agents and the host unnamed message appears, you can change it here. If the agents are running, the value you assign can be overwritten.</p> <p>To force the browser to refresh, save this setting, and press <b>F5</b>.</p>

Parameter	Default value	Descriptions
Authentication Failure Logging	Enabled-Every 3rd Failure	<p>This setting allows you to configure logging criteria for failed authentications. All login types are supported and every login type works independently. The following are valid settings:</p> <ul style="list-style-type: none"> <li>• Enabled-Every Failure—A failed login log entry is recorded after every failed login attempt.</li> <li>• Enabled-Every 2nd Failure—A failed login log entry is recorded after every second failed login attempt.</li> <li>• Enabled-Every 3rd Failure—A failed login log entry is recorded after every third failed login attempt.</li> <li>• Enabled-Every 5th Failure—A failed login log entry is recorded after every fifth failed login attempt.</li> <li>• Disabled—No failed login log entry is recorded.</li> </ul>

Settings (parameters) found on the Services page of the iLO 2 user interface.

Parameter	Default value	Description
Secure Shell (SSH) Access	Enabled	This setting enables you to specify whether the SSH feature on the iLO 2 is enabled or disabled.
Secure shell (SSH) Port	22	This setting enables you to configure the iLO 2 SSH port to be used for SSH communications.
Telnet Access	Disabled	<p>This setting enables you to connect a telnet client to the Remote Console/Telnet port, providing access to the iLO 2 CLP. The following settings are valid:</p> <ul style="list-style-type: none"> <li>• Enabled—iLO 2 enables telnet clients to connect to the Remote Console/Telnet port. Network port scanners can detect that iLO 2 is listening on this port. Unencrypted communication is allowed between the iLO 2 CLP and telnet clients.</li> <li>• Disabled—iLO 2 does not allow telnet clients to connect to the Remote Console/Telnet port. Network port scanners will not normally detect if this port is open on iLO 2. iLO 2 listens on this port for a few seconds when the Remote Console is opened, but telnet connections are not accepted.</li> </ul> <p>Communication between the iLO 2 and Remote Console is always encrypted.</p>
Remote Console/Telnet Port	23	This setting enables you to specify which port the iLO 2 Remote Console uses for remote console communications.
Web Server Non-SSL Port	80	This setting enables you to specify which port the embedded web server in iLO 2 uses for unencrypted communications.
Web Server SSL Port	443	This setting enables you to specify which port the embedded web server in iLO 2 uses for encrypted communications.



Parameter	Default value	Description
Terminal Services Passthrough	Disabled	<p>This setting enables you to control the ability to support a connection through iLO 2 between a Microsoft® Terminal Services client and Terminal Services server running on the host. The following settings are valid:</p> <ul style="list-style-type: none"> <li>• Automatic—When remote console is started, the Terminal Services client is launched.</li> <li>• Enabled—The pass-through feature is enabled and can connect the Terminal Services client directly to the iLO 2 without logging-into the iLO 2.</li> <li>• Disabled—The pass-through feature is off.</li> </ul>
Terminal Services Port	3389	This setting enables you to specify the Terminal Services Port that the iLO 2 uses for encrypted communications with Terminal Services Pass-through software on the server. If the Terminal Services port is configured to anything other than the default, you must manually change the port number.
Virtual Media Port	17988	This setting enables you to specify the port for virtual media support in iLO 2 communications.
Shared Remote Console Port	9300	This setting enables you to specify the Shared Remote Console Port. The Shared Remote Console Port is opened on the client to allow additional users to connect to remote console in a peer-to-peer fashion. This port is only open when Shared Remote Console is in use.
Console Replay Port	17990	This setting enables you to specify the Console Replay Port. The Console Replay Port is opened on the client to enable the transfer of internal capture buffers to the client for replay. This port is only open when a capture buffer is being transferred to the client.
Raw Serial Data Port	3002	This setting specifies the Raw Serial Data port address. The Raw Serial Data port is only open while the WiLODbg.exe utility is being used to debug the host server remotely.

Settings (parameters) found on the Encryption page of the iLO 2 user interface.

Parameter	Default value	Description
Current cipher	—	Displays the current cipher for this web browser session. Upon logging into the iLO 2 using the web browser, the browser and the iLO 2 negotiate the cipher setting to be used for the session. This web page displays the negotiated cipher.
Enforce AES/3DES Encryption	—	<p>This setting allows you to enable or disable AES/3DES encryption.</p> <ul style="list-style-type: none"> <li>• If disabled, AES/3DES encryption is not used.</li> <li>• If enabled, cipher strength must be at least AES or 3DES to connect to iLO 2.</li> </ul>

# Network parameters

Parameter	Default value	Definition
NIC	Yes	This parameter enables the NIC to reflect the state of the iLO 2. The default setting for the NIC is Yes, which is enabled. If DHCP is disabled, you must assign a static IP address to the iLO 2. Assign the IP address using the iLO 2 IP address parameter.
DHCP	Yes	<p>Enables you to select static IP (disabled) or Enables the use of a DHCP server to obtain an IP address for the iLO 2 subsystem.</p> <p>You cannot set the iLO 2 IP address and subnet mask if DHCP is enabled.</p> <p>Enabling DHCP allows you to configure the following DHCP options:</p> <ul style="list-style-type: none"> <li>• Use DHCP Supplied Gateway</li> <li>• Use DHCP Supplied DNS Servers</li> <li>• Use DHCP Supplied WINS Servers</li> <li>• Use DHCP Supplied Static Routes</li> <li>• Use DHCP Supplied Domain Name</li> </ul>
IP address	N/A (DHCP)	Use this parameter to assign a static IP address to the iLO 2 on your network. By default, the IP address is assigned by DHCP.
Subnet mask	N/A (DHCP)	Use the subnet mask parameter to assign the subnet mask for the default gateway. By default, the subnet mask is assigned by DHCP.
Gateway IP address	N/A (DHCP)	Use the gateway parameter to assign the IP address of the network router that connects the iLO 2 subnet to another subnet where the management console resides. By default, the gateway is assigned by DHCP.
iLO 2 subsystem name	iLO 2XXXXXXXXXX X, where the 12 Xs are the server serial number (assigned at the factory)	The iLO 2 comes preset with a DNS/WINS name. The DNS/WINS name is "iLO 2" plus the serial number of the server. This name also is displayed on the tag attached to the bracket of iLO 2. You can change this value.
Domain name	N/A (DHCP)	Enter the name of the domain in which iLO 2 participates. By default, the domain name is assigned by DHCP.
Link	Automatic	Configures the duplex of the network transceiver.

## Network DHCP/DNS parameters

Parameter	Default value	Definition
DHCP	Enabled	Enables you to select static IP (disabled) or enables the use of a DHCP server to obtain an IP address for iLO 2 subsystem. You cannot set the iLO 2 IP address and subnet mask if DHCP is enabled. Enabling DHCP allows you to configure the following DHCP options: <ul style="list-style-type: none"> <li>• Use DHCP Supplied Gateway</li> <li>• Use DHCP Supplied DNS Servers</li> <li>• Use DHCP Supplied WINS Servers</li> <li>• Use DHCP Supplied Static Routes</li> <li>• Use DHCP Supplied Domain Name</li> </ul>
IP Address	N/A (DHCP)	Use this parameter to assign a static IP address to iLO 2 on your network. By default, the IP address is assigned by DHCP.
Domain Name	N/A (DHCP)	Enter the name of the domain in which iLO 2 will participate. By default, the domain name is assigned by DHCP.
Use DHCP supplied gateway	Enabled	Toggles whether the iLO 2 will use the DHCP server-supplied gateway. If not, enter one in the Gateway IP Address box.
Use DHCP supplied DNS servers	Enabled	Toggles whether iLO 2 will use the DHCP server-supplied DNS server list. If not, enter one in the Primary/Secondary/Tertiary DNS Server boxes.
Use DHCP supplied WINS servers	Enabled	Toggles whether iLO 2 will use the DHCP server-supplied WINS server list. If not, enter one in the Primary/Secondary WINS Server boxes.
Use DHCP supplied static routes	Enabled	Toggles whether iLO 2 will use the DHCP server-supplied static route. If not, enter one in the Static Route #1, #2, #3 boxes.
Use DHCP supplied domain name	Enabled	Toggles whether iLO 2 will use the DHCP server-supplied domain name. If not, enter one in the Domain Name box.
WINS Server Registration	Enabled	The iLO 2 automatically registers with a WINS server. By default, WINS server addresses are assigned by DHCP.
DDNS Server Registration	Enabled	The iLO 2 automatically registers with a DNS server. By default, DNS server addresses are assigned by DHCP.
Ping gateway on startup	Disabled	This option causes iLO 2 to send four ICMP echo request packets to the gateway when iLO 2 initializes. This option ensures that the ARP cache entry for iLO 2 is current on the router responsible for routing packets to and from iLO 2.
Domain name	N/A (DHCP)	Enter the name of the domain in which iLO 2 participates. By default, the domain name is assigned by DHCP.
DHCP server	N/A (DHCP)	This setting is automatically detected if DHCP is set to Yes. You cannot change this setting.
Primary, secondary, and tertiary DNS server	N/A (DHCP)	Use this parameter to assign a unique DNS server IP address on the network. By default, the primary, secondary, and tertiary DNS servers are assigned by DHCP.

Parameter	Default value	Definition
Primary and secondary WINS server	N/A (DHCP)	Use this parameter to assign a unique WINS server IP address on the network. By default, the primary and secondary WINS servers are assigned by DHCP.
Static routes #1, #2, #3	N/A for both the destination and gateway address (DHCP)	Use this parameter to assign a unique static route destination and gateway IP address pair on the network. Up to three static route pairs can be assigned. By default, the static routes are assigned by DHCP.
<i>Blade server parameters</i>		
Diagnostic port configuration parameters		
Transceiver speed autoselect	Yes	Toggles the ability of the Transceiver to auto-detect the speed and duplex of the network on the Diagnostic Port. Speed and Duplex are disabled if Autoselect is set to Yes.
Speed	N/A (autoselect)	Configures the speed of the Diagnostic Port. This speed must match the speed of the Diagnostic Port network. If the Autoselect option is set to Yes, the speed will be automatically configured by iLO 2.
Duplex	N/A (autoselect)	Configures the duplex of the Diagnostic Port. The duplex should match the duplex of the Diagnostic Port network. If the Autoselect option is set to Yes, the duplex will be automatically configured by iLO 2.
IP address	192.168.1.1	The Diagnostic Port IP address. If DHCP is being used, the Diagnostic Port IP address is automatically supplied. If not, enter a static IP address here.
Subnet mask	255.255.255.0	The subnet mask for the Diagnostic Port IP network. If DHCP is being used, the Subnet Mask is automatically supplied. If not, enter the subnet mask for the network.

## SNMP/Insight Manager settings parameters

Parameter	Default Value	Definition
SNMP alert destination(s)	No	Enter the IP address of the remote management PC that will receive SNMP trap alerts from the iLO 2. Up to three IP addresses can be designated to receive SNMP alerts.
Enable iLO 2 SNMP alerts	No	The iLO 2 alert conditions are detected by the iLO 2 and are independent of the host server operating system. These alerts can be Insight Manager SNMP traps. These alerts include major events, such as remote server power outages or server resets. They also include the iLO 2 events, such as security disabled or failed login attempt. The iLO 2 forwards the alerts to an HP SIMconsole using the destinations provided.

Parameter	Default Value	Definition
Forward Insight Manager Agent SNMP alerts	No	When set to Yes, these alerts are generated by the Insight Management agents, which are provided for each supported network operating system. The agents must be installed on the host server to receive these alerts. These alerts are sent to HP SIM clients on the network and are forwarded asynchronously by the iLO 2 to the IP addresses that have been configured to receive them.
Enable SNMP pass-thru	Yes	The Enable SNMP pass-through option enables the system to pass SNMP packets from the Insight Management Agent. When set to No, all SNMP traffic is stopped and will not pass-through the iLO 2.
Insight Manager Web Agent URL		The Insight Manager Web Agent URL option enables you to enter the IP address or the DNS name of the host server on which the Insight Manager Web Agents are running. Entering this data in the field provided enables iLO 2 to create a link from the iLO 2 Web pages to the pages of the Web Agent.
Level of data returned	Medium	The Level of Data Returned option regulates how much data is returned to an anonymous request for the iLO 2 information from HP SIM. All settings, except the None Data Level, provide sufficient data to allow integration with HP SIM. The Medium and High settings enable HP SIM and Systems Insight Manager to associate the management processor with the host server. The None Data Level prevents the iLO 2 from responding to the HP SIM requests.

## Directory settings parameters

Parameter	Default value	Definition
Disable directory authentication	No	This parameter enables or disables directory authentication. If directory support is properly configured, this enables user login to iLO 2 using directory credentials.
Schema-free directory	Yes	This parameter enables or disables the use of schema-free directories.
Use HP extended schema	No	This parameter enables or disables the use of extended schema directories.
Enable local user accounts	Yes	This option enables a user to log in using a local user account instead of a directory account. By default, this setting is Enabled.
Directory server address	0.0.0.0	This parameter specifies the Directory Server DNS name or IP address. HP recommends using a DNS name or multi-host DNS name. If an IP address is used, the directory will not be available if that server is down.

Parameter	Default value	Definition
Directory server LDAP port	636	This option sets the port number used to connect to the directory server. The SSL-secured LDAP port number is 636.
LOM object distinguished name		This option specifies the unique name for the iLO 2 in the directory. LOM Object Distinguished Names are limited to 256 characters.
LOM object password		<p>This parameter specifies the password for the iLO 2 object to access the directory. LOM Object Passwords are limited to 39 characters.</p> <hr/> <p><b>NOTE:</b> At this time, the LOM Object Password field is not used. This field is to provide forward compatibility with future firmware releases.</p> <hr/>
LOM object password confirm		Prevents mistyped passwords. If you change the LOM Object Password, also enter the new password in this field.
Directory user context 1, directory user context 2, ... up to directory user context 15		<p>This parameter enables you to specify up to 15 searchable contexts used to locate the user when the user is trying to authenticate using the directory. Directory User Contexts are limited to 128 characters each. Directory User Contexts enable you to specify directory user containers that are automatically searched when an iLO 2 login is attempted. This eliminates the requirement of entering a fully distinguished user name at the login screen. For example, the search context, "ou=lights out devices,o=corp" would allow the user "cn=manager,ou=lights out devices,o=corp" to login to iLO 2 using just "manager." Active Directory allows an additional search context format, "@hostname" for example, "@directory.corp."</p>

## BL p-Class parameters

Parameter	Default value	Definition
Rack name	Provided by rack	The rack name is used to logically group together the components that compose a single rack. When changed, the rack name is communicated to all other components connected in a rack. The name is used when logging and alerting to assist in identifying the component.
Enclosure name	Provided by rack	The enclosure name is used to logically group together the server blades that compose a single enclosure. When changed, the enclosure name is communicated to all other server blades connected in the same enclosure. The name is used when logging and alerting to assist in identifying the component.

Parameter	Default value	Definition
Bay name		The bay name is used when logging and alerting to assist in identifying a component or its function.
Bay	Provided by rack	The Proliant BL p-Class enclosure can support one to eight server blades. The bays are numbered from left to right starting with 1 and finishing with 8. The bay number is used to assist in physically identifying the faulty server blade or other error conditions. This information is for viewing only.
Rack serial number	Provided by rack	The rack serial number identifies the components in the rack as a logical grouping. The serial number is determined during power-up of the various components to create a unique rack serial number. Switching components (server blade enclosure or power supplies) alters the rack serial number.
Enclosure serial number	Provided by rack	The enclosure serial number identifies the particular server blade enclosure in which a server blade resides.
Blade serial number	Provided by blade server	The blade serial number identifies the serial number for the server blade product.
Power source	Rack provides power	<p>The server blade enclosure can be installed in a rack by using one of two configurations:</p> <ul style="list-style-type: none"> <li>• The server blade power supplies can be used to convert normal AC facility power to 48 V DC to power the rack. In this configuration, select the power source as <b>Rack Provides Power</b>. This setting enables each server blade, enclosure, and power supply to communicate power requirements to ensure proper power consumption without risking power failures.</li> <li>• If the facility can provide 48 V DC power directly, without the need for the provided power supplies, then select <b>Facility Provides 48V</b>. Each server blade will not be required to communicate with the infrastructure for power when powering on or off.</li> </ul> <hr/> <p><b>NOTE:</b> It is essential that proper power sizing requirements be performed to ensure sufficient power for all the server blades and other components of the rack.</p> <hr/>
Enable automatic power on	On	Each server blade can be configured to automatically power on when inserted into the enclosure. Depending on the Power Source setting, the server blade communicates with the rack to determine if enough power is available to power on. If the power is available, then the server blade automatically powers on and begins the normal server booting process.

Parameter	Default value	Definition
Enable rack alert logging (IML)	On	As the server blade receives alerts, these events can be logged to the IML. You can view these events by using the iLO 2 System Status—IML tab. Additional IML viewing tools are available to allow viewing from the installed operating system on the server blade.

## iLO Advanced Pack License Key

The iLO 2 Advanced Pack License Key option is used to enable the iLO 2 Advanced Features including Graphical Remote Console, virtual media (floppy and CD-ROM), and directory support . Enter the 25-character key in this field to enable the features.



---

# Technical support

## HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage (<http://welcome.hp.com/country/us/en/wwcontact.html>).

For HP technical support:

- In the United States, for contact options see the Contact HP United States webpage ([http://welcome.hp.com/country/us/en/contact\\_us.html](http://welcome.hp.com/country/us/en/contact_us.html)). To contact HP by phone:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (<http://www.hp.com/hps>).
- In other locations, see the Contact HP worldwide (in English) webpage (<http://welcome.hp.com/country/us/en/wwcontact.html>).

## Before you contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Product identification number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

---

# Acronyms and abbreviations

## ASCII

American Standard Code for Information Interchange

## ASM

Advanced Server Management

## ASR

Automatic Server Recovery

## BMC

baseboard management controller

## CA

certificate authority

## CGI

Common Gateway Interface

## CLI

Command Line Interface

## CLP

command line protocol

## CR

Certificate Request

## DAV

Distributed Authoring and Versioning

## DDNS

Dynamic Domain Name System

## DHCP

Dynamic Host Configuration Protocol

## DLL

dynamic link library

## DNS

domain name system

## DSA

Digital Signature Algorithm

## EMS

Emergency Management Services

## EULA

end user license agreement

## FEH

fatal exception handler

## FSMO

Flexible Single-Master Operation

## GUI

graphical user interface

## HB

heartbeat

## HPONCFG

HP Lights-Out Online Configuration utility

## HPQLOMGC

HP Lights-Out Migration Command Line

## ICMP

Internet Control Message Protocol

## IIS

Internet Information Services

## iLO

Integrated Lights-Out

## IML

Integrated Management Log

## IP

Internet Protocol

## IPMI

Intelligent Platform Management Interface

## ISIP

Enclosure Bay Static IP

## JVM

Java Virtual Machine

## KCS

Keyboard Controller Style

## LAN

local-area network

## LDAP

Lightweight Directory Access Protocol

## LED

light-emitting diode

## LOM

Lights-Out Management

## LSB

least significant bit

## MAC

Media Access Control

## MLA

Master License Agreement

## MMC

Microsoft® Management Console

## MP

Multilink Point-to-Point Protocol

## MTU

maximum transmission unit

## NIC

network interface controller

## NMI

non-maskable interrupt

## NVRAM

non-volatile memory

## PERL

Practical Extraction and Report Language

## PKCS

Public-Key Cryptography Standards

## POST

Power-On Self Test

## PSP

ProLiant Support Pack

## RAS

remote access service

## RBSU

ROM-Based Setup Utility

## RDP

Remote Desktop Protocol

## RIB

Remote Insight Board

## RIBCL

Remote Insight Board Command Language

## RILOE

Remote Insight Lights-Out Edition

## RILOE II

Remote Insight Lights-Out Edition II

## RSA

Rivest, Shamir, and Adelman public encryption key

## RSM

Remote Server Management

## SLES

SUSE Linux Enterprise Server

## SMASH

System Management Architecture for Server Hardware

## SMS

System Management Server

## SNMP

Simple Network Management Protocol

## SSH

Secure Shell

## SSL

Secure Sockets Layer

## TCP

Transmission Control Protocol

## UART

universal asynchronous receiver-transmitter

## UID

unit identification

## USB

universal serial bus

VM

Virtual Machine

VPN

virtual private networking

WINS

Windows® Internet Naming Service

WS

web services

XML

extensible markup language

---

# Index

## A

- ADD\_USER 64, 73, 74
- administration 46, 157
- authentication, WS-Management 9
- authorized reseller 169

## B

- BL p-Class blade parameters 166
- blade commands, CLP 30
- blade commands, RIBCL 119
- blade information 30
- boot commands 31
- boot commands, CLP 31
- boot commands, RIBCL 141

## C

- certificate, settings 109
- CERTIFICATE\_SIGNING\_REQUEST 109
- CGI helper scripts 57
- CGI, software components 57
- CLEAR\_EVENTLOG 84
- CLI, commands 10
- CLP base commands 12
- CLP, blade commands 30
- CLP, boot commands 31
- CLP, connection options 10
- CLP, directory settings 23
- CLP, embedded health settings 20
- CLP, escape commands 12
- CLP, eventlog commands 30
- CLP, firmware updates 29
- CLP, iLO 2 commands 19
- CLP, LED commands 32
- CLP, license commands 23
- CLP, miscellaneous commands 35
- CLP, multi-user support 10
- CLP, network commands 16
- CLP, SNMP settings 22
- CLP, specific commands 13
- CLP, start and reset commands 27
- CLP, system target and properties settings 32
- CLP, user commands 14

- CLP, using 10
- CLP, virtual media commands 25
- COLD\_BOOT\_SERVER 141
- command block, 145
- command block, DIR\_INFO 113
- command block, LOGIN 72
- command block, RACK\_INFO 119
- command block, RIB\_INFO 81
- command block, SERVER\_INFO 126
- command block, USER\_INFO 72
- command line mode 10
- command-line parameters, HPONCFG 63
- commands, base 12
- commands, blade 30
- commands, directory 23
- commands, network 16
- commands, user 14
- commands, virtual media 25
- commands, WS-Management 9
- compatibility, WS-Management 9
- COMPUTER\_LOCK\_CONFIG 84, 85
- configuration procedures 64, 65, 66
- configuration utilities 61
- configuration, capturing 67
- configuration, obtaining complete configuration 64
- configuration, obtaining specific information 65
- configuration, restoring 67
- configuration, setting a configuration 66
- contacting HP 169
- CPQLOCFG.EXE, batch processing 48
- CPQLOCFG.EXE, parameters 49
- CPQLOCFG.EXE, runtime errors 46
- CPQLOCFG.EXE, syntax errors 46

## D

- data types 70
- data types, RIBCL 70
- dedicated NIC, re-enabling 154
- DELETE\_CURRENT\_USER 75, 76
- DELETE\_SERVER 150, 151
- DELETE\_USER 75
- DIR\_INFO command block 113
- directory services 165
- directory settings 165



- directory settings, CLP 23
- directory settings, parameters 165
- directory settings, RIBCL 113, 114, 116
- domain name system (DNS) 49, 52, 64, 86, 87, 117
- Dynamic Host Configuration Protocol (DHCP) 64, 86, 87
- dynamic link library (DLL) 61

## E

- EJECT\_VIRTUAL\_MEDIA 106
- embedded health settings, CLP 20
- embedded health settings, RIBCL 128
- enclosure, IP settings 122, 123
- eventlog commands, CLP 29
- eventlog commands, RIBCL 82, 84
- events, WS-Management 9
- examples, RIBCL 70

## F

- features, IPMI 2.0 8
- features, new 7
- features, SSH 41
- firmware update, CLP 29
- firmware update, RIBCL 100, 101
- F-keys 40

## G

- GET\_ALL\_USERS 79
- GET\_ALL\_USERS\_INFO 80
- GET\_DIAGPORT\_SETTINGS 120
- GET\_DIR\_CONFIG 114
- GET\_EMBEDDED\_HEALTH 128
- GET\_ENCLOSURE\_IP\_SETTINGS 122
- GET\_EVENT\_LOG 82, 83
- GET\_FIRMWARE\_VERSION 101, 102
- GET\_GLOBAL\_SETTINGS 91, 92
- GET\_HOST\_POWER\_REG\_INFO 134
- GET\_HOST\_POWER\_SAVER\_STATUS 132, 133
- GET\_HOST\_POWER\_STATUS 132, 135, 136
- GET\_HOST\_PWR\_MICRO\_VER 136, 137
- GET\_NETWORK\_SETTINGS 86
- GET\_POWER\_CAP 131
- GET\_POWER\_READINGS 130
- GET\_PWREG\_CAPABILITIES 137, 138
- GET\_RACK\_SETTINGS 119
- GET\_SERVER\_AUTO\_PWR 143
- GET\_SERVER\_NAME 127
- GET\_SNMP\_IM\_SETTINGS 98

- GET\_SSO\_SETTINGS 146
- GET\_TOPOLOGY 124
- GET\_TWOFACOR\_SETTINGS 110
- GET\_UID\_STATUS 143, 144
- GET\_USER 76
- GET\_VM\_STATUS 106, 107
- GET\_VPB\_CABLE\_STATUS 144, 145
- global settings 158
- global settings parameters 158
- guidelines, RIBCL 70

## H

- HOLD\_PWR\_BTN 140, 141
- HOTKEY\_CONFIG 102, 103
- HP Lights-Out Migration Command Line (HPQLOMGC) 152, 171
- HP ProLiant Essentials Rapid Deployment Pack 8
- HP SIM parameters 164
- HP SIM, application launch 47
- HP SIM, grouping LOM devices 47
- HP SIM, integration 42
- HP technical support 169
- HPONCFG (HP Lights-Out Online Configuration Utility) 61
- HPONCFG, commands 63
- HPONCFG, iLO 2 configuration examples 64, 65, 66, 67
- HPONCFG, installation 62
- HPONCFG, Linux 62, 63, 64
- HPONCFG, parameters 63
- HPONCFG, requirements 61
- HPONCFG, using 61, 62, 63
- HPONCFG, variable substitution 67
- HPQLOMGC, using 152

## I

- IIS, scripted media 58
- iLO 2 port, re-enabling 154
- iLO 2 settings 19, 152
- iLO 2 settings, CLP 19
- iLO 2 settings, RIBCL 81
- iLO 2 status parameters 156
- iLO ports 154
- ILO\_CONFIG 152
- IMPORT\_CERTIFICATE 109, 110
- IMPORT\_SSH\_KEY 115, 116
- importing SSH keys, PuTTY 43
- INSERT\_VIRTUAL\_MEDIA 104, 105
- installation, Linux server 62

- installation, Windows server 62
- Intelligent Platform Management Interface (IPMI) 8
- Internet Information Services Manager 58
- introduction 7
- IP settings, enclosure 122, 123
- IPMI (Intelligent Platform Management Interface) 8

## K

- KCS (Keyboard Controller Style) 8
- key map, VT100 37
- Keyboard Controller Style (KCS) 8

## L

- LED commands, CLP 32
- LICENSE 104
- license commands, CLP 23
- license commands, RIBCL 104
- license parameters 168
- Linux sever installation 62
- Linux, F-key codes 40
- LOGIN command block 72

## M

- management port 154
- MOD\_BLADE\_RACK 124, 125, 126
- MOD\_DIAGPORT\_SETTINGS 120, 121
- MOD\_DIR\_CONFIG 116, 117, 118
- MOD\_ENCLOSURE\_IP\_SETTINGS 123, 124
- MOD\_GLOBAL\_SETTINGS 93, 96, 98
- MOD\_NETWORK\_SETTINGS 64, 87, 89, 91
- MOD\_SNMP\_IM\_SETTINGS 99, 100
- MOD\_SSO\_SETTINGS 147, 148
- MOD\_TWOFACOR\_SETTINGS 111, 112, 113
- MOD\_USER 73, 77, 78, 79
- Mxagentoconfig 43

## N

- network settings parameters 162, 163
- network settings, CLP 16
- network settings, RIBCL 86, 87

## O

- online configuration utility 61
- OpenSSH utility 42
- operating systems supported 61
- operational overview 70
- overview, CLP 10
- overview, CPQLOCFG.EXE 46

- overview, guide 7
- overview, HPONCFG 61
- overview, IPMI 8
- overview, Lights-Out Configuration Utility 46
- overview, Perl scripting 51
- overview, RIBCL 70
- overview, SSH 41
- overview, telnet 36
- overview, virtual media scripting 55

## P

- parameter definitions 156
- Perl, sending XML scripts 53
- Perl, SSL connection 52
- Perl, using 51
- Perl, XML enhancements 51
- phone numbers 169
- properties, system 32
- PuTTY utility 42
- PuTTY, importing SSH keys 43

## R

- RACK\_INFO command block 119
- Remote Insight Board Command Language (RIBCL) 70
- RESET\_RIB 82
- RESET\_SERVER 139, 140
- response definition, RIBCL 71
- RIB\_INFO command block 81
- RIBCL command block 71
- RIBCL, data types 70
- RIBCL, DIR\_INFO commands 113
- RIBCL, examples 70
- RIBCL, LOGIN command 72
- RIBCL, RACK\_INFO commands 119
- RIBCL, response definitions 71
- RIBCL, RIB\_INFO commands 81
- RIBCL, SERVER\_INFO commands 126
- RIBCL, SSO\_ 145
- RIBCL, string 70, 71
- RIBCL, USER\_INFO commands 72

## S

- script body, XML 51
- scripting interface, perl 51
- scripting, virtual media 55
- scripts 51, 52, 53, 61, 62, 63, 70
- Secure Shell (SSH) 41
- Secure Sockets Layer (SSL) 9, 52, 53

- server identification 156
- server status 156
- server status parameters 156
- SERVER\_AUTO\_PWR 142, 143
- SERVER\_INFO command block 126
- SERVER\_NAME 127
- SET\_HOST\_POWER 133, 136
- SET\_POWER\_CAP 131
- SET\_VM\_STATUS 107, 109
- setup, scripted 51
- shared network port, enabling 154
- shared network port, features 154
- shared ports 154
- SNMP parameters 164
- SNMP settings, CLP 22
- SNMP settings, RIBCL 98, 99
- SSH key authorization 42
- SSH key authorization, tool definition files 43
- SSH keys, importing 43, 45
- SSH utility 42
- SSH, connection 42
- SSH, features 41
- SSH, overview 41
- ssh-keygen 45
- SSL connection, opening 52
- SSL, WS-Management 9
- SSO\_INFO 145
- SSO\_SERVER 149, 150
- start and reset commands, CLP 27
- start and reset commands, RIBCL 82, 139, 140, 141
- status, WS-Management 9
- string, RIBCL 70, 71
- support 169
- supported key sequences 37, 103
- supported operating systems 61
- system status 156
- system target information, CLP 32
- system target information, RIBCL 126
- system, targets 32

## T

- technical support 169
- telephone numbers 169
- telnet 36
- telnet, command set 36
- telnet, key sequences 37
- telnet, security 37
- telnet, using 36
- topology, RIBCL commands 124

- two-factor authentication, settings 110, 111

## U

- UID\_CONTROL 144
- UPDATE\_RIB\_FIRMWARE 100, 101
- user account, adding 70
- user administration parameters 157
- user settings, CLP 14
- user settings, RIBCL 72
- USER\_INFO command block 72

## V

- variable substitution, HPONCFG 67
- virtual media commands, CLP 25
- virtual media commands, RIBCL 104, 106, 107
- virtual media image files 57
- virtual media scripting, CGI helper 57
- virtual media scripting, IIS requirements 58
- virtual media scripting, Linux 56
- virtual media scripting, using 55
- virtual media scripting, web server requirements 55
- VT100 key map 37
- VT100, F-key codes 40

## W

- WARM\_BOOT\_SERVER 141, 142
- Windows server installation 62

## X

- XML (Extensible Markup Language) 51, 70
- XML header 53, 70
- XML query, unauthenticated 46
- XML, general guidelines 51, 70